Colección Recursos Informáticos

Redes informáticas

Nociones fundamentales

(Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6, ...)

5ª edición

José DORDOIGNE





INFORMÁTICA TÉCNICA

Redes informáticas

Nociones fundamentales (4ª edición)

Este libro sobre redes se dirige tanto a **principiantes** que quieran conocer las redes informáticas, como a informáticos **más experimentados** que deseen reforzar y actualizar sus conocimientos.

Se presentan los **principios básicos** (normas, arquitecturas comunes, cableado, cifrado de datos, topología, redes inalámbricas, interconexión de redes…) y los **diferentes protocolos** existentes en las redes informáticas (Ethernet, Wi-Fi, Bluetooth, ADSL, WiMax…) desde un punto de vista operativo, sin confundir al lector en un discurso demasiado teórico.

Se examina la configuración de red para **Windows**, **Linux**, **Mac OSX** y**Android**. La parte dedicada al almacenamiento se presenta de manera detallada explicando claramente los términos **NAS, SAN, zoning, Fiber Channel, FCoE e iSCSI**; igualmente se describen los protocolos de replicaciones entre bahías. Se explica en detalle el funcionamiento de la**deduplicación para las copias de seguridad** así como los **WAFS**.

Así mismo, se muestra un resumen sobre la **virtualización** que permite al lector comprender los problemas, ventajas e inconvenientes de las diferentes soluciones del mercado. También se abordan las tecnologías **ATM y otras conexiones de tramas**.

Desde un punto de vista del hardware de red, se explica el **algoritmo de Spanning tree**, así como el funcionamiento de **VSS**. Respecto al enrutamiento, se revisan los **protocolos RIP**, **OSPF y BGP**, así como**HSRP**. Se presentan en detalle los **protocolos TCP/IP**: en particular la descomposición en sub-redes en IPv4, así como un nuevo enfoque completo del **direccionamiento IP v6** (incluyendo VoIP). Se examinan igualmente los **servicios de red como DHCP, DNS, NTP o SNMP**. Un capítulo trata de los principios básicos de seguridad frente a las amenazas que pueden afectar a una red.

El anexo proporciona una lista de los **acrónimos** más significativos en el mundo de las redes informáticas.

Los capítulos del libro:
Prólogo – Presentación de los conceptos de red – Estandarización de protocolos – Transmisión de los datos en la capa física – Software de comunicación – Arquitectura de red e interconexión – Capas bajas de las redes personales y locales – Protocolos de redes MAN y WAN – Protocolos de capas medias y altas – Principios de protección de una red – Reparación de una red – Anexos

---

José DORDOIGNE

Ingeniero informático, consultor especializado en sistemas y redes de una gran consultora, **José Dordoigne** tiene numerosas certificaciones; Microsoft (MCSE NT4, 2000, 2003 y MC ITP Enterprise Administrator 2008), Linux (Red Hat Certified Engineer y LPI 101) y Cisco (CCNA). Su destreza pedagógica y técnica se reconoce a través de una experiencia de casi 9 años como formador, de más de 6 años como consultor y auditor de numerosas empresas, así como con la escritura de varios libros sobre los Sistemas operativos Microsoft, redes y TCP/IP.

Prólogo

Las redes constituyen un amplio campo que suele ser difícil de comprender porque se trata de un conocimiento que implica múltiples y complejos campos técnicos que trabajan en direcciones divergentes.

Aunque para el aprendizaje de nuevos conceptos o la consolidación de los conocimientos ya adquiridos la complejidad es una dificultad importante, el hecho de descomponer los problemas, y de añadir muchas ilustraciones, permite abordar estos conocimientos con más facilidad.

Esto es lo que hemos intentado hacer en este libro, cuyo objetivo es entender los principios que rigen las redes informáticas actuales, usando en la medida de lo posible enfoques pragmáticos y visuales.

Este libro se dirige a cualquier persona usuaria de informática y que quiera adquirir conocimientos sobre el tema o dirigirse al mundo de las redes.

Examinemos juntos los diferentes capítulos que componen este libro y el enfoque que hemos adoptado para tratar los diversos temas propuestos.

El primer capítulo aborda los principales conceptos de redes, incluyendo el concepto de recursos compartidos, para permitir al lector tomar perspectiva sobre los distintos temas y vincularlos con sus propias experiencias pasadas como usuario informático de red. También se desarrolla la virtualización, que hoy en día no se puede ignorar, para entender los diferentes conceptos subyacentes, identificar los desafíos, ventajas e inconvenientes de cada una de las soluciones: tanto si se trata de la virtualización del sistema operativo cliente o servidor, como de la virtualización de sesión o incluso de la virtualización de aplicación que introduce el concepto de aplicación como servicio (*Software as a Service*).

La complejidad de las redes viene del hecho de que se mezclan a la vez componentes de software y de hardware y de que el acceso a los recursos es sistemáticamente crítico para las empresas. Este primer capítulo permite también al lector familiarizarse con los diferentes mecanismos de tolerancia a errores existentes.

El siguiente capítulo propone en primer lugar una primera aproximación teórica al modelo de capas de red OSI y, a continuación, una interpretación pragmática basada en ejemplos concretos de protocolos. Esto sirve para entender el papel que juega cada una de las capas de red. Se pone una atención especial en el conocimiento de la red local Ethernet y el funcionamiento de las capas TCP/IP. El objetivo es medir el papel de los identificadores de cada nivel, así como las decisiones que se toman en el direccionamiento de los datos. No nos hemos dejado el nivel de aplicación, y se ha tratado específicamente el concepto de modo conectado.

Una sección sobre los organismos de normalización permite conocer las entidades que han marcado las normativas para las redes y, sobre todo, proporciona direcciones de sitios web para que quienes quieran profundizar en los múltiples temas abordados en este libro puedan buscar información complementaria.

El siguiente capítulo, ampliamente detallado, permitirá entrar en el meollo del tema, concentrándose en la transmisión de datos, los dispositivos, los tipos de conexiones, con la ayuda de numerosas ilustraciones. Se tratan la conversión de datos a través de la codificación, el soporte de transmisión que se utiliza, así como el método de acceso al canal que permite compartir el soporte. Se revisan los diferentes soportes (con cables o inalámbricos) para explicar los principios de funcionamiento y entender en qué medida es posible emitir y recibir simultáneamente datos.

El siguiente capítulo propone ejemplos de ilustración de configuración de red TCP/IP en los sistemas operativos clientes más generalizados.

En el siguiente capítulo, se habla de la arquitectura de red y la interconexión. Se trata de entender las diferencias esenciales entre conmutador y enrutador y de comprender globalmente la función de los componentes de interconexión. Se examinan más a fondo los métodos de acceso al soporte, para conocer profundamente Ethernet y Token Ring, que son los dos protocolos históricos de redes.

El capítulo sobre las capas bajas permitirá analizar más específicamente las normas y características asociadas a la mayor parte de los protocolos LAN.

En el siguiente capítulo se exponen los protocolos MAN y WAN que se pueden encontrar en las empresas o que tuvieron un papel histórico en el pasado.

En el capítulo que trata de los protocolos de las capas medias y altas, se pone énfasis en el protocolo IP: tanto en la versión 4 como en la versión 6. Se exponen explicaciones detalladas, que tratan de la descomposición en subredes en IPv4, de la categorización, el alcance, la notación, los túneles o la autoconfiguración en IPv6. Se trata también la VoIP, así como las principales aplicaciones conocidas en TCP/IP.

A continuación, un capítulo sobre los principios de protección permite familiarizarse con las amenazas actuales y los principales medios para defenderse desde un punto de vista personal o en un contexto empresarial (cortafuegos, DMZ, proxy, etc).

Por último, en el capítulo final sobre la reparación de redes se revisan los problemas más comunes y las herramientas más usuales para identificar los errores.

Finalmente, se explican las conversiones binaria, decimal y hexadecimal para permitir trabajar más fácilmente con las direcciones IPv4 o v6.

Antecedentes

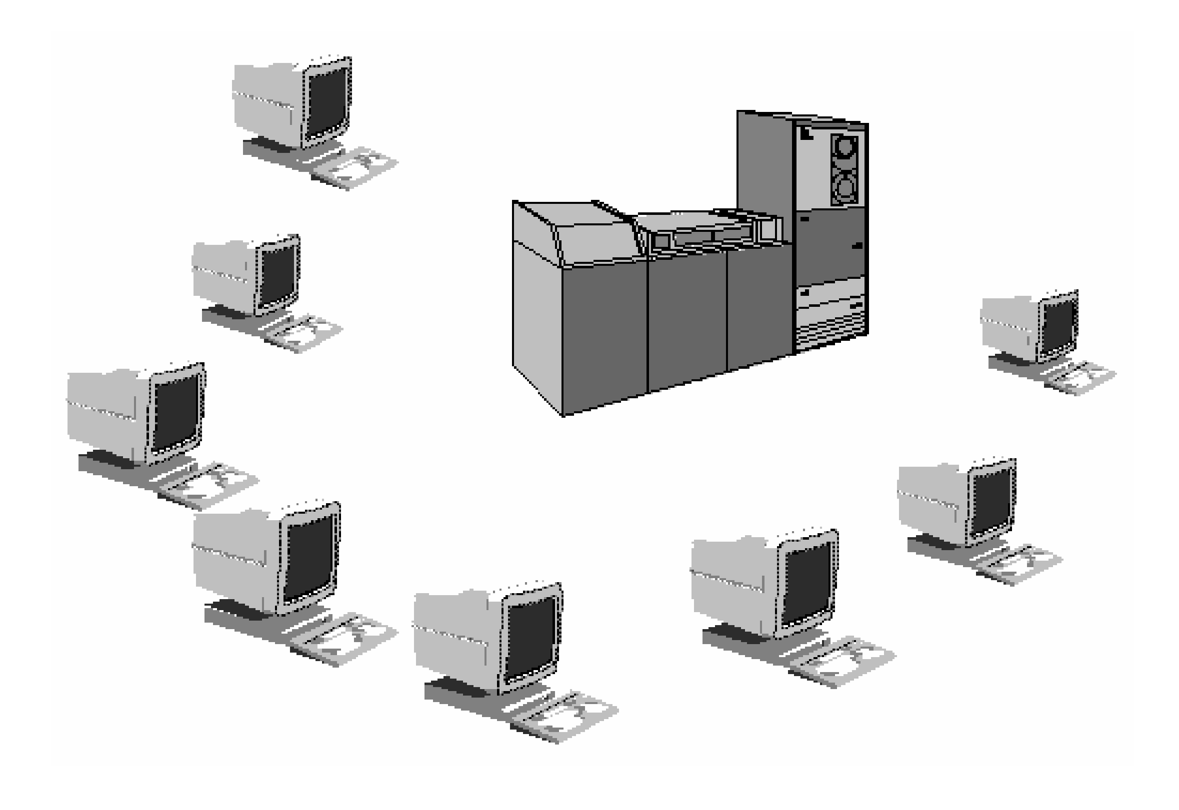
Gracias a la evolución de las capacidades de las redes, el tratamiento automatizado de la información ha mejorado considerablemente en los últimos cincuenta años. A partir de los grandes sistemas propietarios centralizados, hoy están disponibles varias arquitecturas.

1. Principios de la informática de redes

a. La informática centralizada

En los años cincuenta y sesenta, los datos se administraban con grandes sistemas u ordenadores centrales, accesibles a partir de puestos externos, origen de los terminales. Con pantallas y teclados muy simples, se utilizaban los equipos de comunicación que permitían el intercambio de caracteres con el sistema central.

Esta forma de compartir información y servicios es el origen de las redes que conocemos hoy en día.

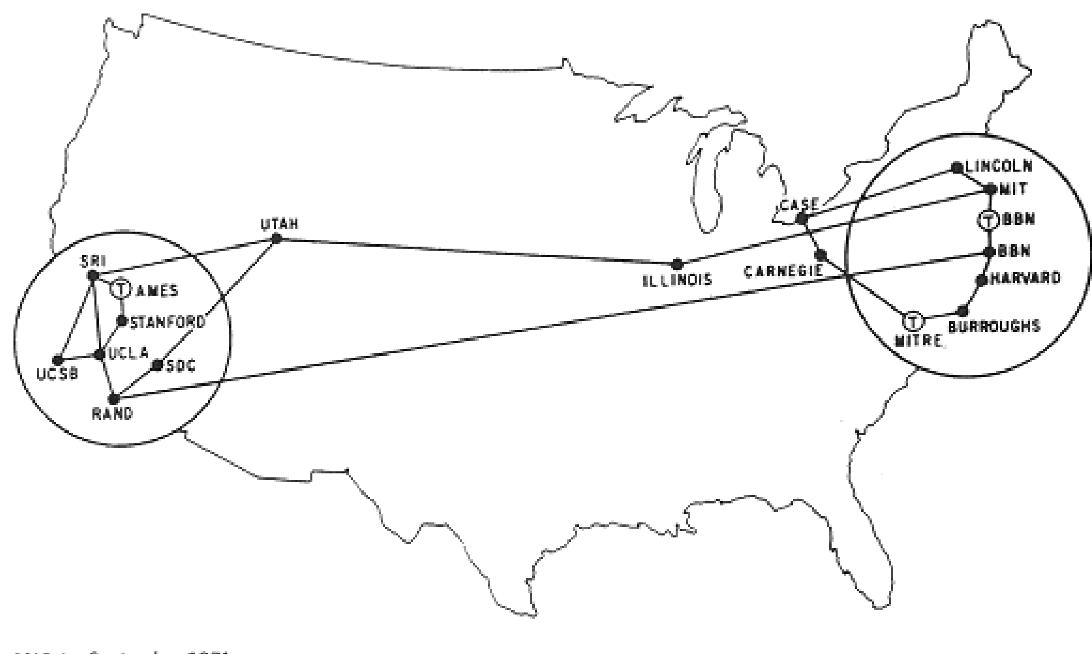


Terminales y mainframe

Las redes DECnet de DIGITAL y de IBM (SNA - *System Network Architecture*) constituyen ejemplos de redes de arquitectura centralizada.

b. La primera red informática a gran escala

A finales de los años sesenta, se llega a la conclusión de que los recursos están globalmente mal utilizados. Se considera que fue el clima de guerra fría lo que condujo al departamento de defensa estadounidense (DoD - *Department of Defense*) a desarrollar protocolos y equipos con el fin de disponer de una red con alta tolerancia a fallos (en caso de guerra). Por ello, nace en 1970 la red ARPANET (*Advanced Research Project Agency NETwork*). Con este hecho, la utilización de las líneas telefónicas existentes constituye un primer punto de apoyo que desempeñará un papel esencial en el futuro desarrollo de Internet.



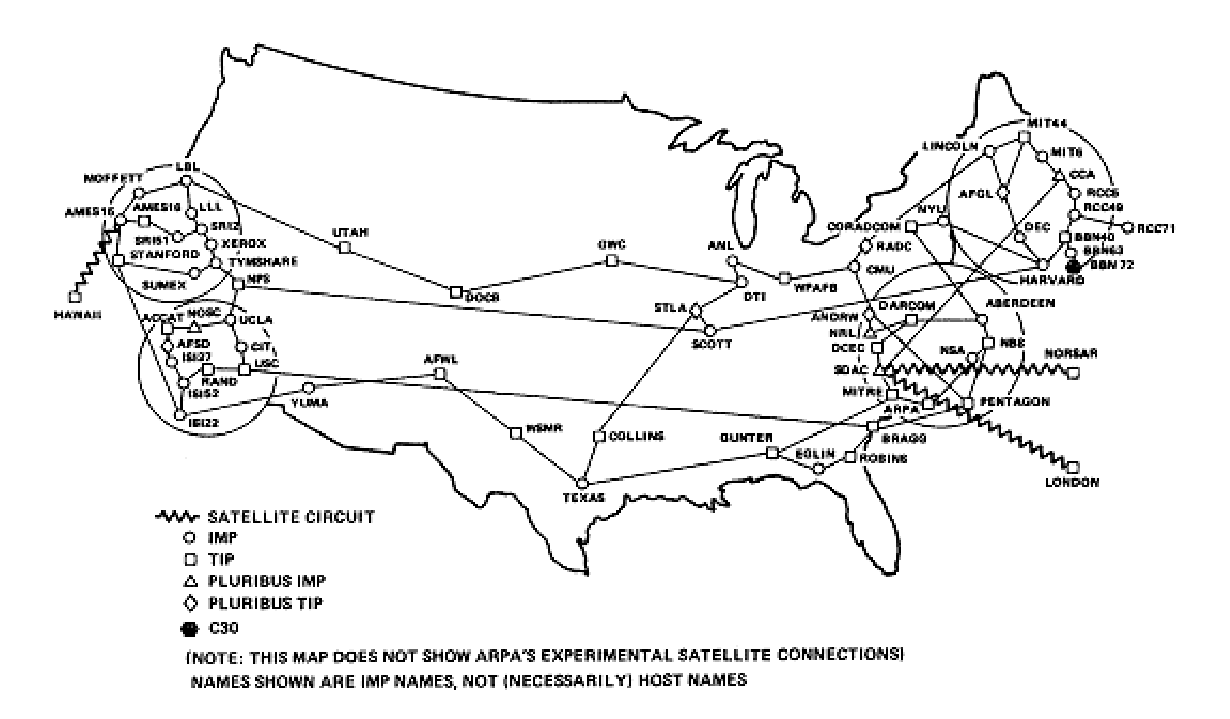
MAP 4 September 1971

ARPANET experimentó un crecimiento muy rápido. El diagrama anterior muestra su situación en septiembre de 1971.

En 1972, se cuentan una cuarentena de instituciones conectadas entre sí que disponen de los servicios de correo electrónico y conexión a distancia.

El siguiente mapa representa la situación de ARPANET en octubre de 1980, que ya incluye la conexión vía satélite, por paquetes, con Londres.

ARPANET GEOGRAPHIC MAP, OCTOBER 1980



c. El desarrollo de una norma de hecho: TCP/IP

A mediados de los años setenta, ARPANET adopta un nuevo modo de comunicación con el*Transmission Control Protocol/Internet Protocol* (TCP/IP).

En 1980, la agencia DARPA, que administraba ARPANET, decide dejar de considerar secreto militar

el TCP/IP. Al mismo tiempo, los sistemas operativos UNIX continúan su extraordinario desarrollo. La versión UNIX *Berkeley Software Development* (BSD) proporciona gratuitamente a las universidades incluso los códigos fuente TCP/IP. A partir de entonces, la red mundial no ha dejado de crecer, y toma el nombre de **Internet** en su versión no militar.

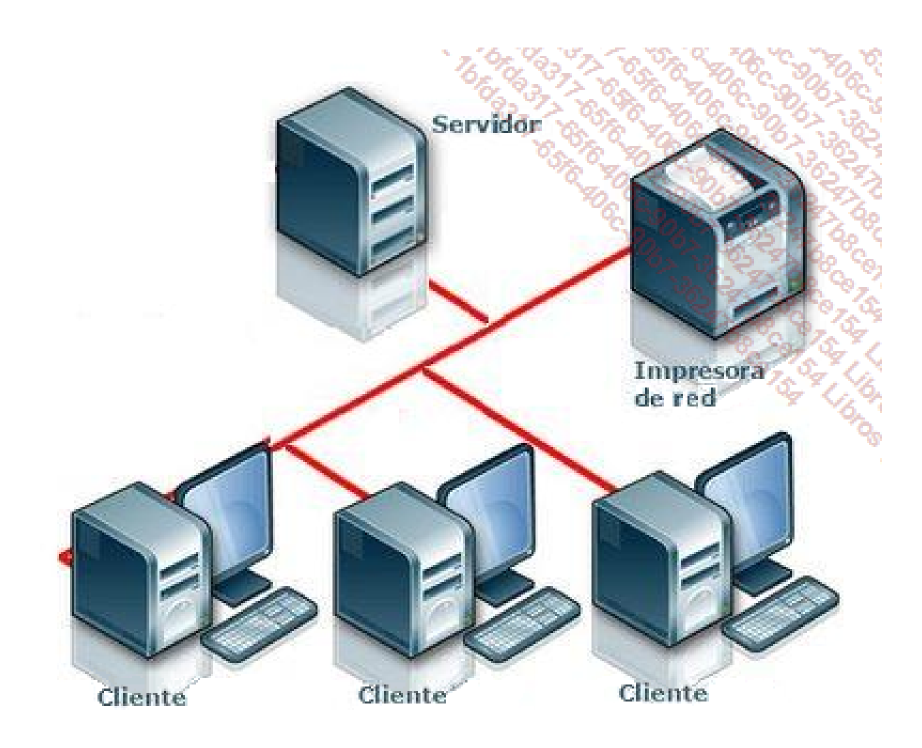
d. La informática descentralizada

El concepto de ordenador personal aparece con el primer PC (*Personal Computer*) de IBM, el PC XT, en 1981.



PC XT en 1981

La llegada de los PC condujo a la creación de un nuevo enfoque en la gestión de la información: la informática descentralizada.



Arquitectura cliente/servidor

El tratamiento global se distribuye en subprocesos repartidos en distintas estaciones. La distribución de la información se garantiza con los servicios de red que permiten disponer de las mismas funcionalidades en todas las estaciones.

Aparece el concepto de redes pequeñas, seguido por el de redes locales LAN.

2. Redes heterogéneas

Progresivamente se desarrollan normas que permiten simplificar la interconexión de sistemas heterogéneos. Organismos como el *Institute of Electrical and Electronics Engineers* (IEEE) proponen normas para los protocolos de capas físicas.



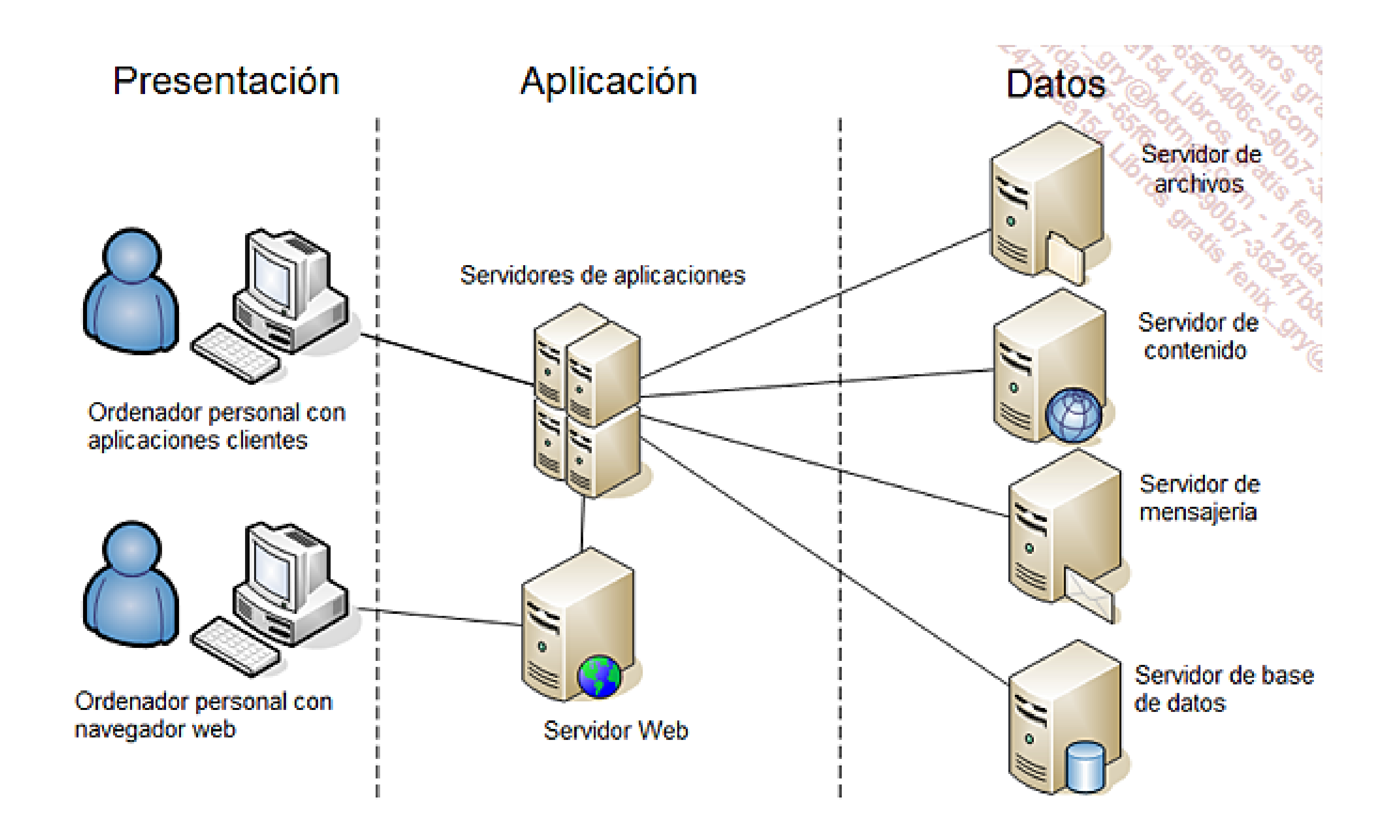
Sitio Web: ieee.org

3. Redes informáticas actuales

Hoy en día, las redes están constituidas por ordenadores y sistemas operativos heterogéneos, que a menudo se interconectan a través de Internet.

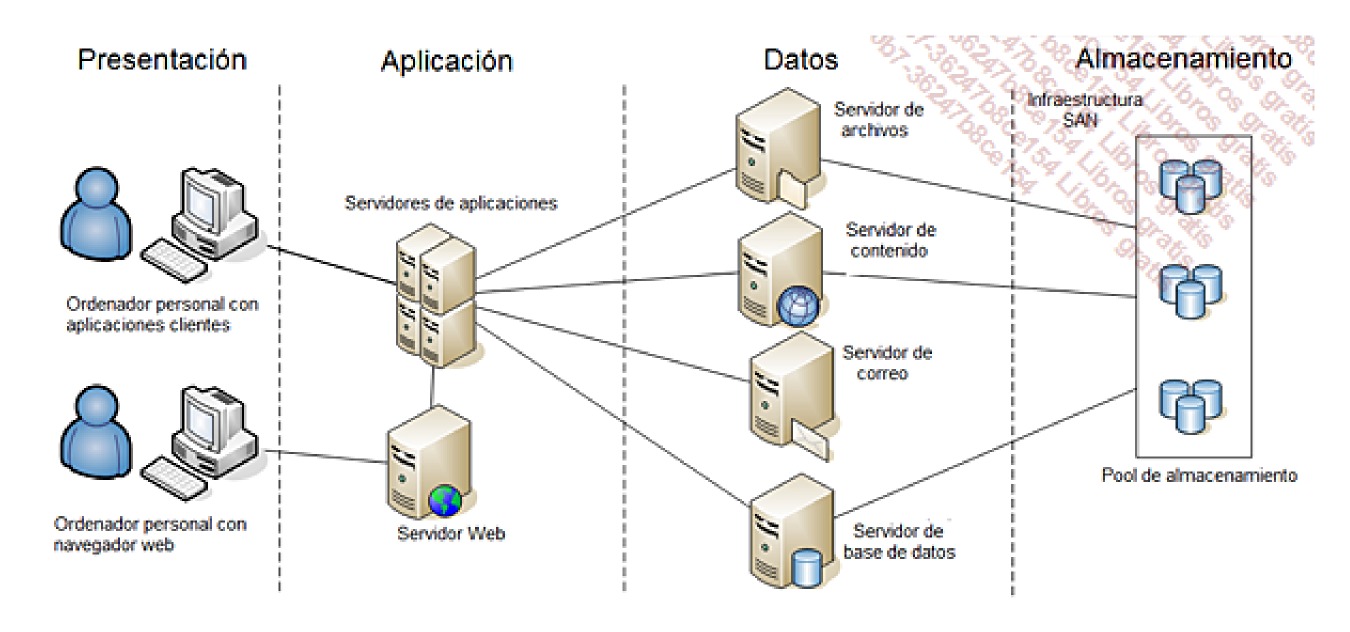
La distribución de recursos se multiplica a través de arquitecturas que incluyen diferentes capas (*tiers*, que significa capa o nivel en inglés). Los recursos de que dispone el usuario se emplean para organizar la información recibida cuando una capa intermedia administra las aplicaciones. Estas se han vuelto independientes de los datos y se distribuyen en distintos niveles.

El siguiente esquema representa una arquitectura de tres capas (3 *tiers*) o 3/3.



Arquitectura 3/3

Con la utilización de una infraestructura SAN, esta arquitectura puede incluso contener una capa adicional y, por ejemplo, llegar a 4 capas.



Arquitectura 4/3

Principales elementos de una red

En esta parte, definiremos los términos indispensables para una buena comprensión del entorno de red. Mencionaremos las diferencias fundamentales entre las redes organizadas en torno a servidores y las redes que funcionan entre pares. Veremos en qué casos utilizar cada uno de los dos sistemas.

1. Desde la perspectiva del software

a. Principios

El sistema operativo de red es un sistema complejo compuesto por diferentes capas lógicas (protocolos de comunicación, capa de aplicación...). Permite a varias personas interconectadas (físicamente) trabajar con los mismos recursos.

Proporciona un control de acceso a la red (seguridad de conexión, seguridad en el acceso a los recursos) coordinando al mismo tiempo los accesos simultáneos (administra a menudo colas de espera para los dispositivos exclusivos).

b. Definiciones

Desde un punto de vista del software, los ordenadores conectados a una red se dividen en dos categorías en función de las acciones que efectúan sobre esta.

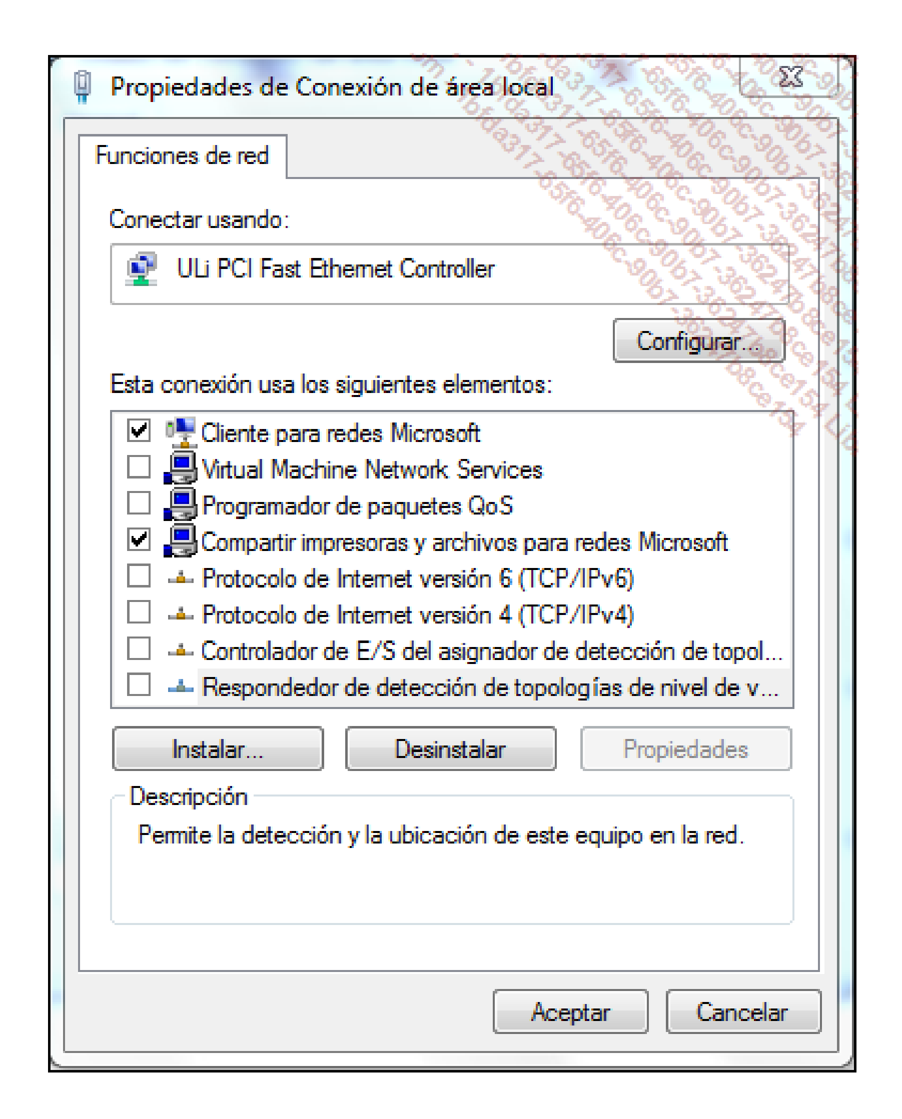
Un *cliente* es el solicitante de servicios. Puede ser, por ejemplo, un puesto de trabajo de usuario que solicita servicios de aplicaciones, de archivos, de impresión...

Estos servicios los ofrece una entidad lógica llamada *servidor*.

Los sistemas operativos de red son capaces de pedir u ofrecer servicios. Por el contrario, su orientación principal es diferente, ya que dan prioridad a una u otra posibilidad. Un puesto de trabajo, que no tiene como objetivo principal ofrecer servicios a la red, dispone un sistema que prioriza el aspecto cliente.

En cambio, un sistema operativo de servidor proporciona servicios más eficientes. Es capaz de soportar hardware más avanzado y administrar capacidades (memoria, espacio en disco) más importantes.

Al evolucionar, los sistemas operativos de red han adquirido cierto número de capacidades complementarias. Por ejemplo, todo el software de Windows ofrece servicios de archivos, de impresión y de alojamiento/distribución de sitios Web, sin necesidad de instalar software de terceros. Obviamente, las posibilidades que ofrecen las versiones destinadas a los usuarios finales son bastante más limitadas.



Propiedades de red en un cliente Windows 7: las funcionalidades de cliente (Cliente para redes Microsoft) y de servidor (Compartir...) están activadas.

Un servidor puede estar dedicado o no. Si está dedicado, solo puede ofrecer uno de los servicios habituales. Estas configuraciones son ideales. Permiten dimensionar el hardware en función de las necesidades del servicio. Un servidor de archivos dedicado no tendrá necesidad de un microprocesador potente, al contrario que su aplicación. Para una empresa, dedicar los servidores a una u otra tarea es una solución que suele ser costosa, aunque se mejora la eficacia y la administración.

El aumento de las capacidades y de la potencia de los servidores hace además que se puedan simultanear servicios en una máquina física.

La *virtualización* de servidores aporta una respuesta a esta problemática. Estos programas permiten la simulación de varios servidores virtuales en una única plataforma física.

c. El sistema operativo de red

El sistema operativo de red (NOS - *Network Operating System*) o SOR (Sistema Operativo de Red) es el que, a menudo, condiciona la arquitectura de la red.

Como ejemplos de sistemas operativos, se distinguen los sistemas organizados en torno a un servidor y los basados en una arquitectura de puesto a puesto.

Puesto a puesto

Cuando todos los puestos tienen un papel idéntico y son a la vez clientes de los recursos disponibles y servidores, se habla de red de igual a igual, de par a par (*peer-to-peer*), o también de puesto a puesto. En este tipo de estructura, que en general agrupa pocos puestos, los recursos,

las operaciones de seguridad y las tareas de administración se distribuyen en el conjunto de la red. No puede haber un control centralizado. Generalmente, cada usuario es administrador de su propio puesto. Este tipo de organización implica que los usuarios no sean completamente neófitos y puedan trabajar en un entorno correctamente estructurado.

Otro inconveniente es que no se puede centralizar la gestión de los usuarios en una única base de datos de la red; es decir, no se puede controlar el acceso a los recursos en función de los nombres de los usuarios.

En un entorno de ordenadores cuyo sistema operativo es Microsoft Windows 7 o Windows Vista en sus ediciones no profesionales, hablaremos de grupos de trabajo (*workgroup*).

Red centralizada

Cada usuario dispone de un nombre y una contraseña para identificarse, que debe introducir en el momento de la apertura de una sesión de red. También se centraliza la base de datos de los usuarios de la red.

Así es posible controlar el acceso a los recursos utilizando la seguridad a nivel de usuario: es decir, se individualizan los permisos para cada usuario en función de cada uno de los recursos disponibles. De esta manera, es mucho más fácil saber quién hace qué y en qué momento. Se nombra administrador a un usuario específico que tiene por función administrar el conjunto de los recursos de la red. Es el usuario que tiene más poder sobre el conjunto de la red.

Podemos citar MS Windows 2003 o 2008 como sistemas operativos de arquitectura centralizada.

Seguridad a nivel de recursos

Hablamos de seguridad a nivel de recursos para hacer hincapié en el hecho de que es en los recursos donde se centra la seguridad. Se asignan las contraseñas para los recursos necesarios independientemente de los usuarios.

En un principio, no es necesario darse a conocer utilizando explícitamente el nombre de usuario y la contraseña. Sin embargo, cuando solicitemos el acceso a un nuevo recurso, será necesario precisar que disponemos de los permisos correspondientes. Productos como Windows 7 o Windows Vista en sus diferentes versiones familiares funcionan bajo esta premisa. Las contraseña asociadas a los recursos se guardan para que el usuario no tenga que introducirlos nuevamente cada vez que accede.

Es decir, asociamos permisos específicos a este recurso compartido para permitir accesos regidos por contraseña (independientemente de los usuarios).

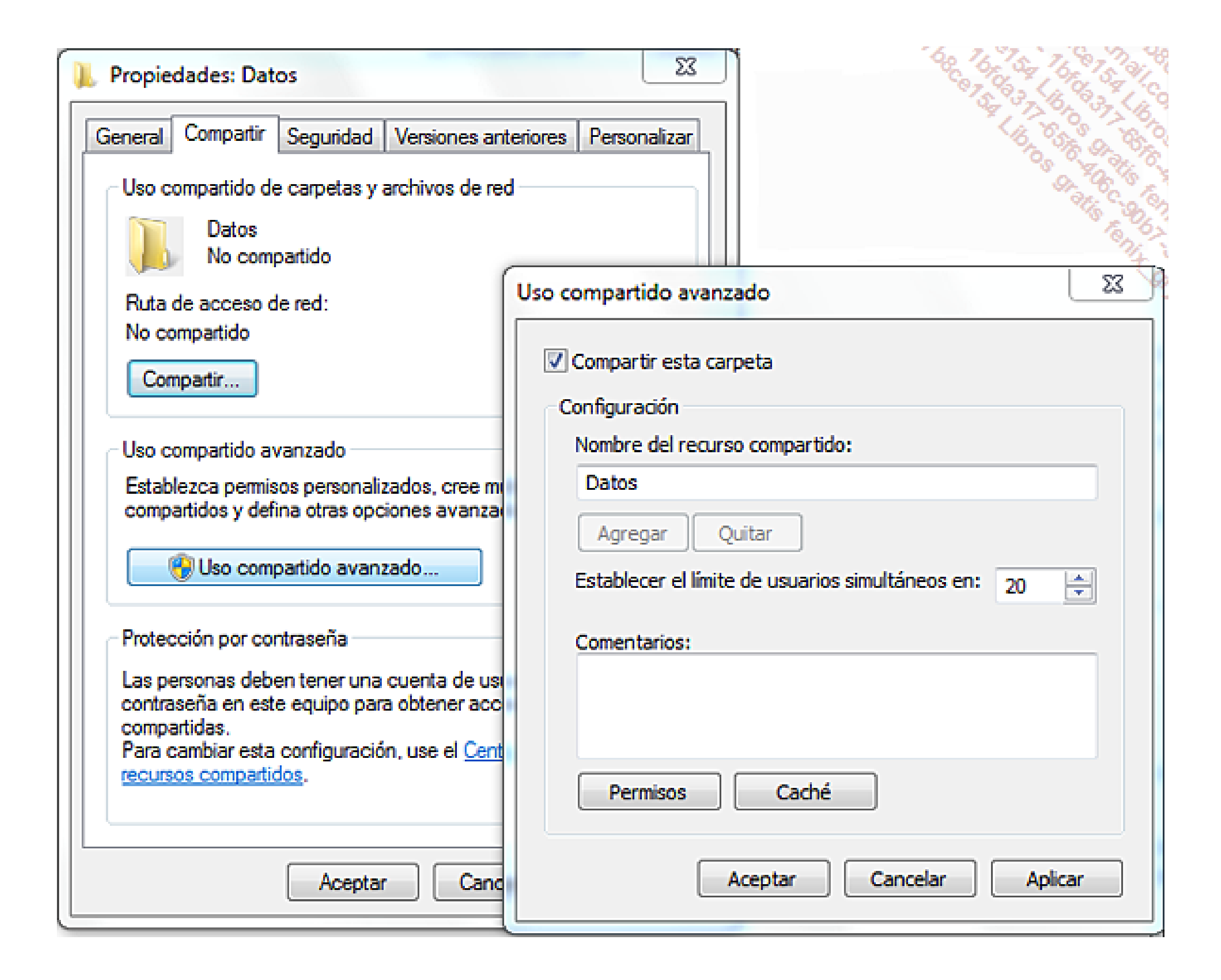

De hecho, si un usuario quiere impedir a otro acceder a su recurso, debe modificar la contraseña e informar al resto de los usuarios (a los que debe permitir el acceso).

Seguridad a nivel de usuario

La seguridad a nivel de usuario, por el contrario, permite asignar permisos más específicos a cada usuario para un recurso dado. Es necesario que antes cada uno se identifique ante una entidad de referencia.

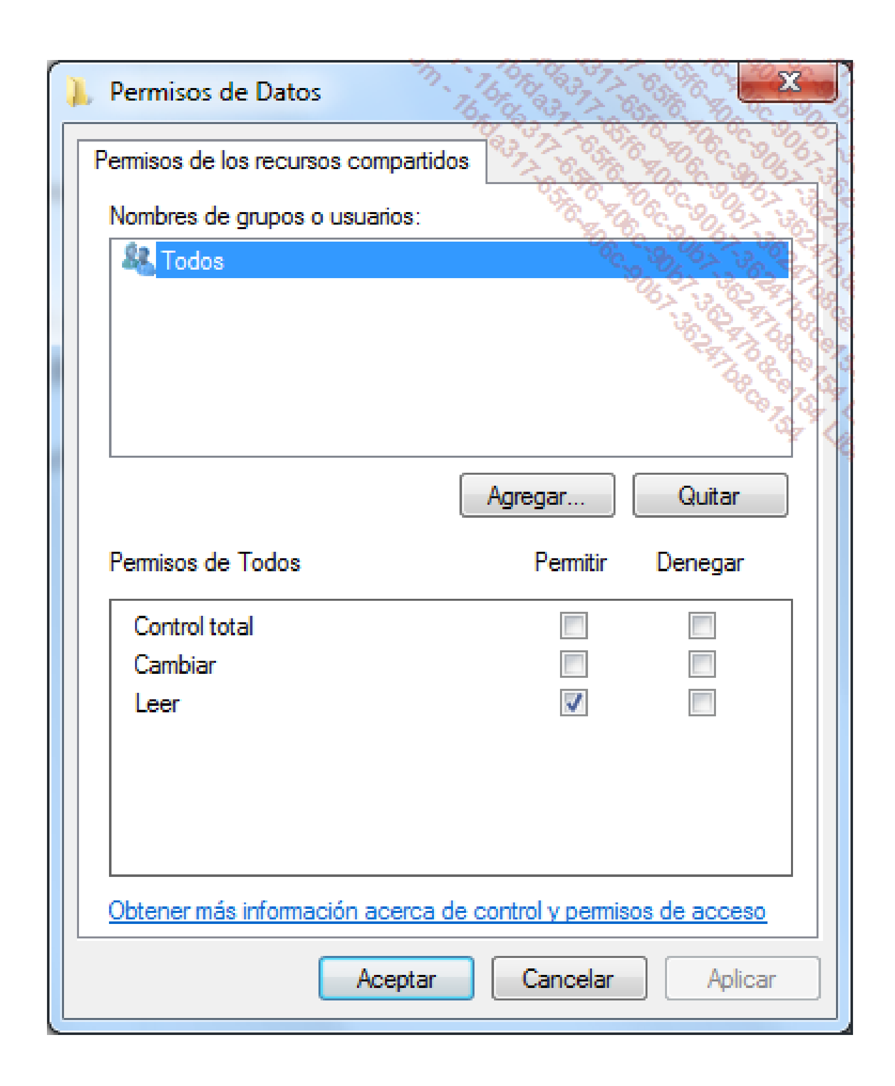
Esta puede ser local (ordenador con MS Windows 7 o Vista) o remota (servidor de cuentas). Es necesario abrir una sesión para autentificarse y así permitir un acceso transparente a los recursos a los cuales el usuario accederá más tarde.

Por ejemplo, para permitir que los usuarios accedan a una carpeta de un sistema MS Windows, en primer lugar es necesario compartirla.



Compartir una carpeta en Windows

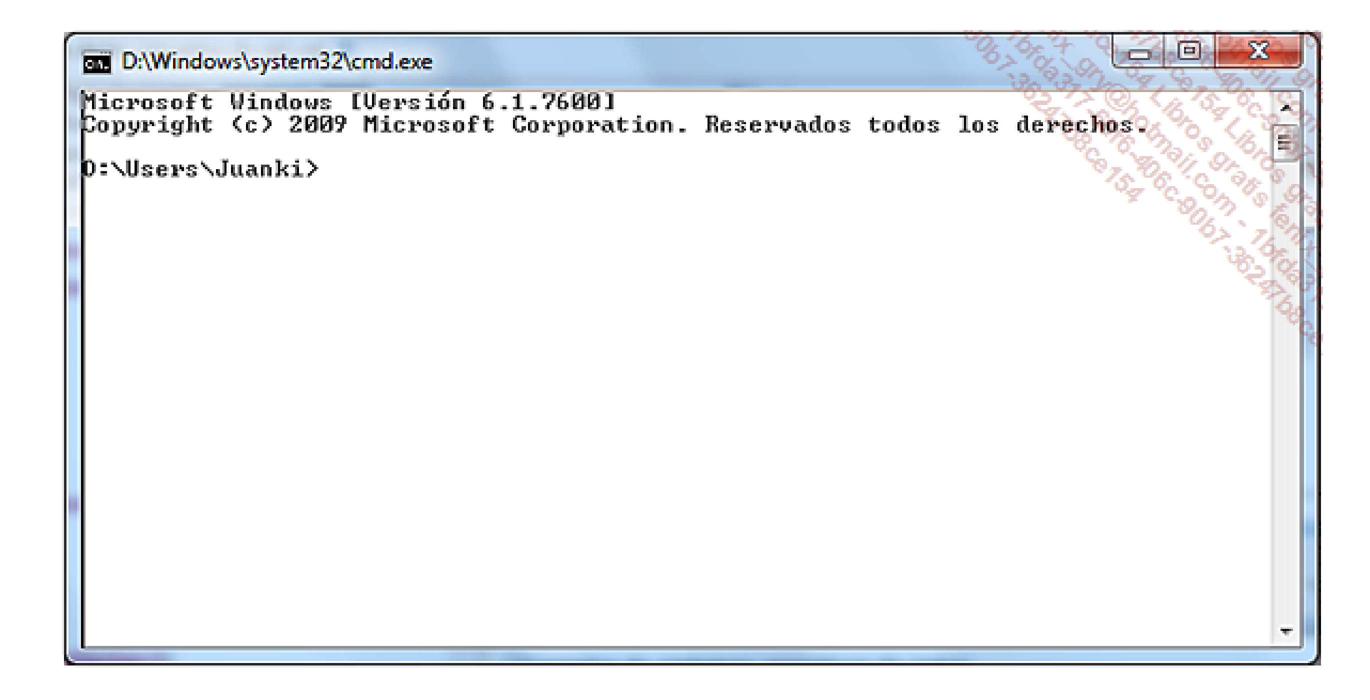
Los permisos de acceso se deben asociar a este recurso compartido en función de las cuentas de usuarios o de su grupo de pertenencia.



Ejemplos de sistemas operativos de redes

Los sistemas operativos de redes de **Microsoft** están separados en dos familias. Windows 2000 Server (NT5.0) y Windows 2003 (NT5.2) son los sucesores de Windows NT4 Server. Para el usuario, Windows 2000 Profesional (NT5.0) y Windows 98 tuvieron como sucesor a Windows XP (NT5.1), en edición familiar o profesional.

La siguiente generación, Windows Vista (núcleo 6.0), ha sido el predecesor de la versión 6.1 del núcleo, con Windows 7 en el puesto de trabajo del usuario.



En el lado del Servidor, encontramos Windows Server 2008 (núcleo 6.0) y Windows Server 2008 R2 (núcleo 6.1).

Finalmente, Windows 8 se basa en el núcleo 6.2, igual que Windows Server 2012.

Los diferentes sistemas de tipo **UNIX** se dedican exclusivamente a tareas de servidor. Se puede citar entre ellos a Sun Solaris, HP-UX, IBM AIX, UNIXWARE...

Linux es un sistema operativo muy importante. La versión del núcleo de Linux permite identificar las funcionalidades que se han añadido.

La primera versión estable que se publicó en marzo de 1994 fue la 1.0. Ofrecía todos los servicios clásicos de un sistema UNIX.

La versión 2.0 se publicó en julio de 1996 con mejoras en la gestión de arquitecturas de muchos más modelos de procesadores, más módulos y una gestión más completa de la red.

En enero de 1999, se lanzó la versión 2.2 que implementaba NTFS e IPv6.

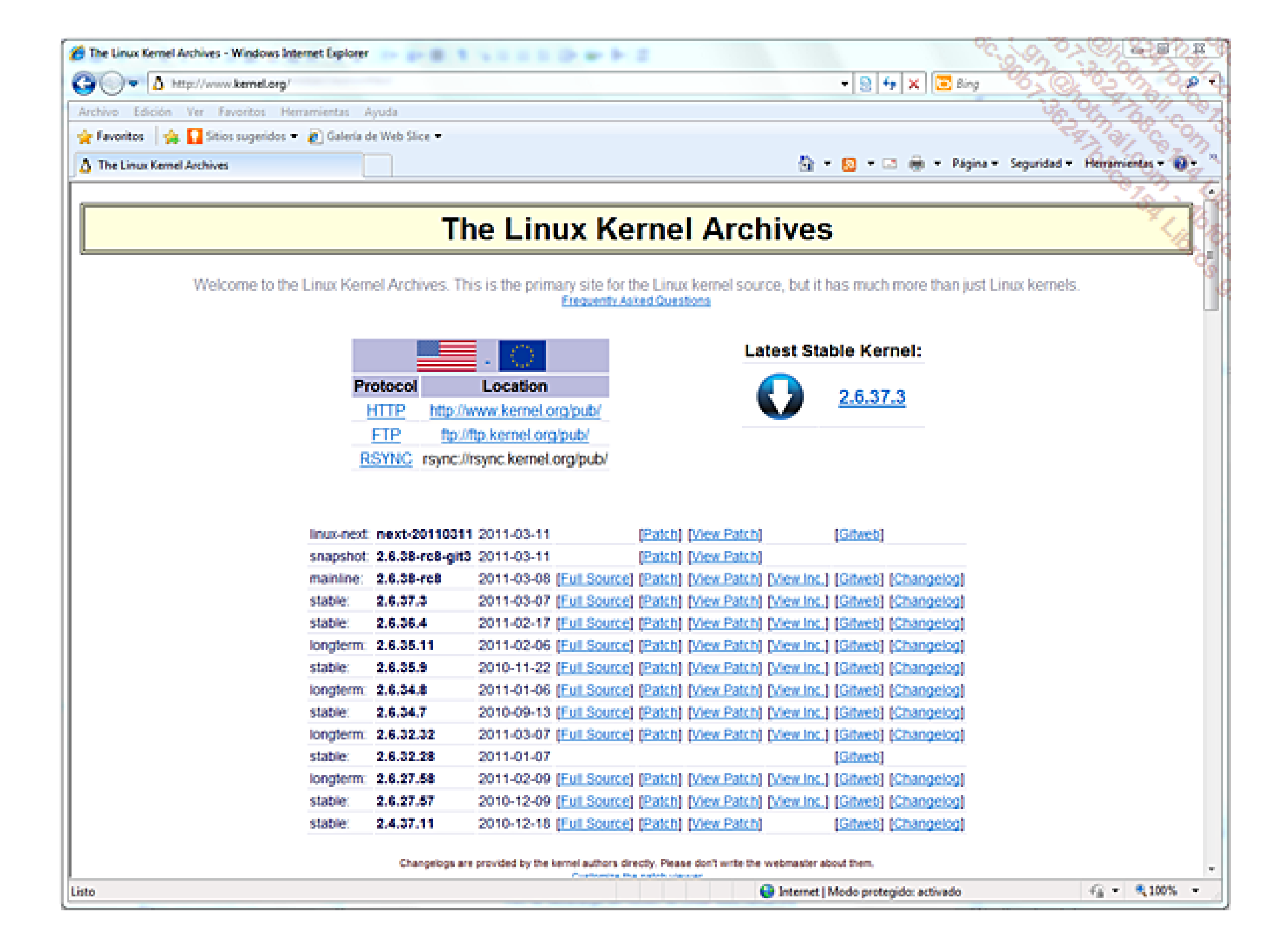
Uno de los aportes importantes de la versión 2.4 que apareció en enero de 2001 fue, entre otros, el soporte de USB, PCMCIA y también NFSv3.

La versión 2.6 se lanzó en diciembre de 2003, y ofreció un verdadero núcleo preemptivo, así como NFSv4.

El soporte de USB 3.0 o la defragmentación en caliente de ext4 han aparecido en la versión 2.6.31 (septiembre de 2009).

La última versión, 3.6.9, ha aparecido en septiembre de 2012.

Observe que, cuando una versión beta se está desarrollando, la segunda cifra del número de versión es impar.



Web de descarga del núcleo de Linux: www.kernel.org

En función de su instalación, Linux puede utilizarse como puesto de trabajo o como servidor.

2. Desde la perspectiva del hardware

a. La interconexión

Para que la comunicación en red sea operativa, en primer lugar es necesario interconectar los equipos entre ellos. Frecuentemente se utiliza una interfaz por cable, como un cable conectado a una tarjeta de red o a un módem. También se puede utilizar la interfaz inalámbrica a través de comunicaciones inalámbricas, que utilizan los infrarrojos, el láser o las ondas de radio.

b. Los protocolos de comunicación

Además del hardware, que garantiza la conectividad y el intercambio de las señales de soporte físico o de ondas, es necesario utilizar normas de comunicación. Estos protocolos permiten dar un sentido a la señal que circula entre las estaciones de trabajo y administrar el acceso al soporte compartido.

Tecnología de redes

El transporte de los datos informáticos por las redes, transparente para los usuarios, es el fruto de tecnologías complejas que ofrecen numerosos y variados servicios. Las nuevas tecnologías de la información y la comunicación (NTIC) permiten una flexibilidad de conexión a las redes a la que Internet no es ajena.

1. Definición de una red informática

Una red es un medio de comunicación que permite a personas o grupos compartir información y servicios.

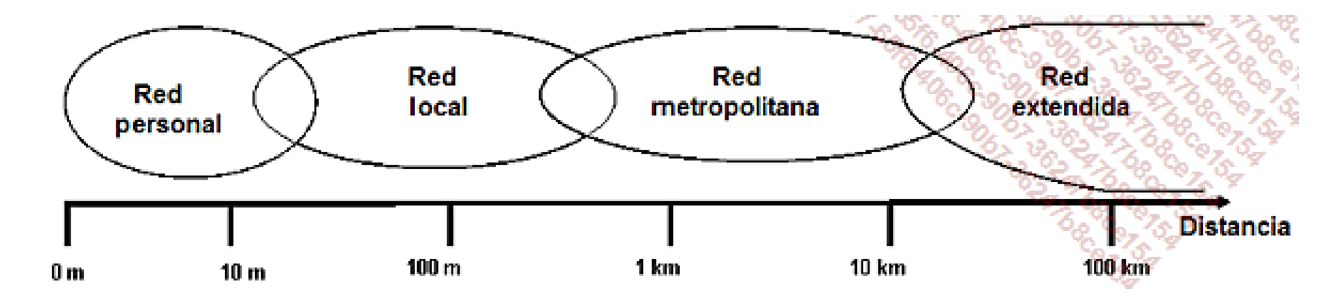
La tecnología de las redes informáticas está compuesta por el conjunto de herramientas que permiten a los ordenadores compartir información y recursos.

Las redes telefónicas forman una generación de redes de telecomunicación que precedió a las de la informática. Desde hace algunos años, se da una convergencia entre estas dos redes. De hecho, las nuevas tecnologías permiten el transporte de voz y datos con los mismos medios.

Una red está constituida por equipos llamados nodos. Las redes se categorizan en función de su amplitud y de su ámbito de aplicación.

Para comunicarse entre sí, los nodos utilizan protocolos, o lenguajes, comprensibles para todos ellos.

2. Topologías de redes informáticas



a. La red personal

El alcance de red más restringido se llama en inglés *Personal Area Network* (PAN). Centrada en el usuario, designa una interconexión de equipos informáticos en un espacio de una decena de metros en torno al usuario, el *Personal Operating Space* (POS). Otros nombres de este tipo de red son: red individual y red doméstica.

b. La red local

De tamaño superior, ya que se extiende hasta algunos centenares de metros, es la *Local Area Network* (LAN), en castellano Red de Área Local. Conecta entre sí ordenadores, servidores... Generalmente se utiliza para compartir recursos comunes, como periféricos, datos o aplicaciones.

c. La red metropolitana

La red metropolitana o *Metropolitan Area Network* (MAN), que también se conoce como red federalista, garantiza la comunicación a distancias más extensas y a menudo interconecta varias redes LAN. Puede servir para interconectar, por una conexión privada o pública, diferentes departamentos, distantes algunas decenas de kilómetros.

d. La red extendida

Las redes con mayor alcance se clasifican como WAN, acrónimo de *Wide Area Network* (WAN). Están compuestas por redes de tipo LAN, o incluso MAN. Las redes extensas son capaces de transmitir la información a miles de kilómetros por todo el mundo. La WAN más famosa es la red pública Internet, cuyo nombre procede de Inter Networking, o interconexión de redes.

3. Compartir recursos

El primer objetivo de las redes es poner recursos en común, garantizando, en particular, que se comparta la información que, en informática, existe bajo distintas formas:

- Archivos.
- Documentos.
- Datos.

Un conjunto de servicios de red aporta las funcionalidades requeridas. A menudo están relacionados por el sistema operativo de red, que dirige la información hacia aplicaciones específicas de los servicios administrados.



Interfaz de Windows 8

a. Los servidores de archivos

Las primeras formas de información dirigidas a través de las aplicaciones de redes son los archivos. Se almacenan en estructuras de carpetas (Windows) o directorios (UNIX/Linux).

Un archivo contiene datos de formas diferentes que se presentan de manera libre, no estructurada.

Los servidores de archivos efectúan cuatro funciones esenciales:

- almacenamiento;
- transferencia y copia;
- sincronización;
- salvaguarda y archivado...

Almacenamiento de archivos

Ante el rápido aumento del volumen de datos gestionados, se ha inventado un gran número de unidades de almacenamiento en línea (soportes fijos), sin conexión (soportes extraíbles) y en sistema combinado (banco de discos), como por ejemplo: discos magnéticos, ópticos, magneto-ópticos, discos duros, llaves USB, DVD-Rom...).

El almacenamiento centralizado permite optimizar al máximo equipos que suelen ser costosos. Además, la unidad de almacenamiento puede elegirse según las necesidades, el tiempo de acceso, la fiabilidad y la vida útil del soporte.

Los datos más antiguos y los menos utilizados se pueden transferir desde soportes costosos hacia soportes más económicos y que tienen una vida útil más prolongada.

La información contenida en los archivos almacenados se puede compartir fácilmente gracias a la red. Evidentemente, los sistemas garantizan la seguridad de los accesos, ya sea mediante la aplicación que administra el intercambio de archivos o mediante el propio sistema de archivos.

Transferencia y copia de archivos

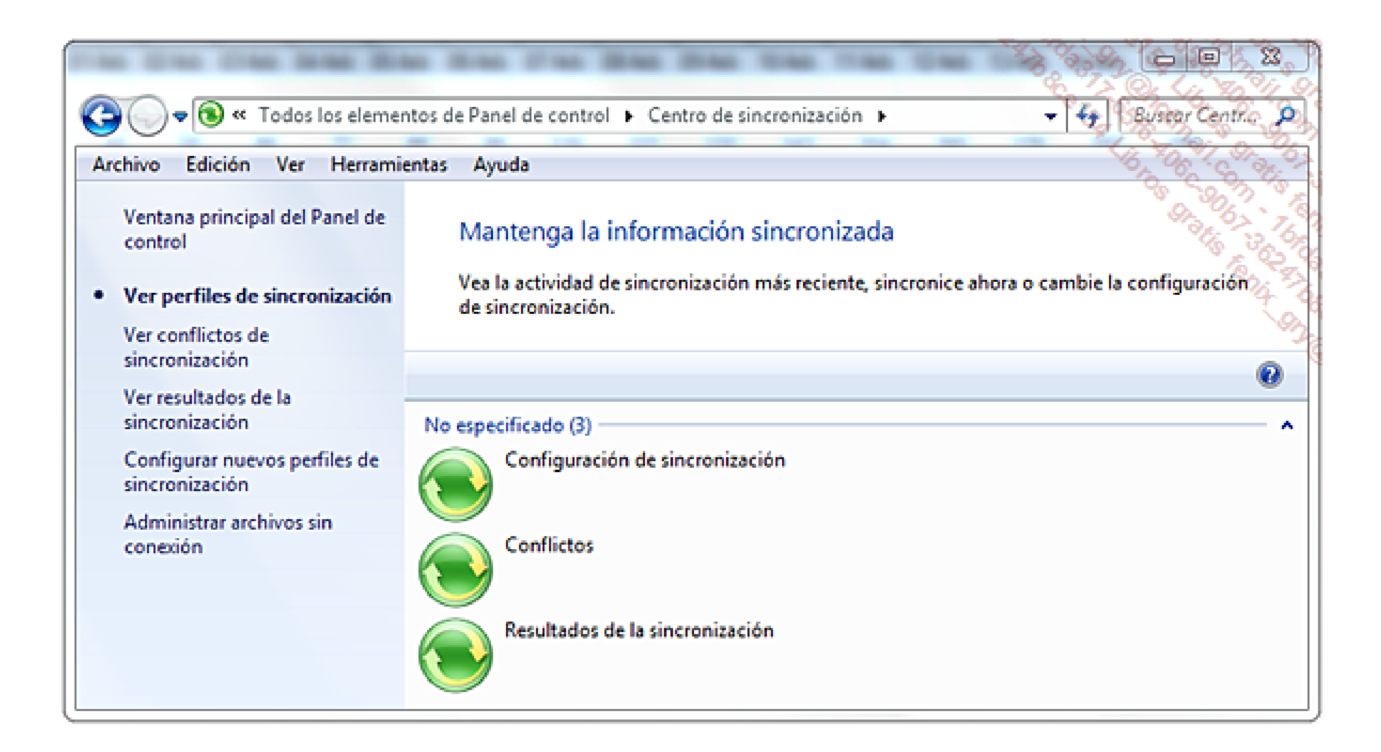
Antes de la implementación de soluciones informáticas para el intercambio de archivos, los usuarios recurrían a medios de comunicación extraíbles para trasladar su información.

Gracias a los servicios de redes, se facilita enormemente el intercambio de información. Trasladar o copiar archivos entre ordenadores (puestos de trabajo o servidores) es muy sencillo.

Sincronización de archivos

El aumento del número de ordenadores portátiles y de dispositivos móviles ha originado un nuevo problema para las empresas. La sincronización de los datos modificados fuera de la empresa, sin conexión, debe estar garantizada en el momento en que se establece de nuevo la reconexión con los servidores. Este servicio debe, además, tener en cuenta las modificaciones simultáneas.

En efecto: puede que un usuario haya modificado la versión del archivo en el servidor mientras que otro ha hecho lo mismo en su ordenador portátil, sin conexión a la red. Por lo tanto, cuando se registra una modificación y se almacena con posterioridad en el servidor, la última copia sustituye a la última versión del documento. Por ello es esencial, para disponer de la versión más reciente, saber en qué momento tuvieron lugar las últimas modificaciones. Esto es lo que permite la función de sincronización de las actualizaciones de archivos. Esta función debe ser capaz de combinar inteligentemente las distintas copias existentes (se utilizan las fechas y las horas).



Centro de sincronización de Windows 7

Archivado y copias de seguridad

Con el fin de prevenir la desaparición de archivos (por errores en el manejo o avería del material de almacenamiento), es necesario establecer una estrategia de archivado, en un soporte en línea o fuera de línea. De esta manera podremos disponer rápidamente de copias de seguridad.

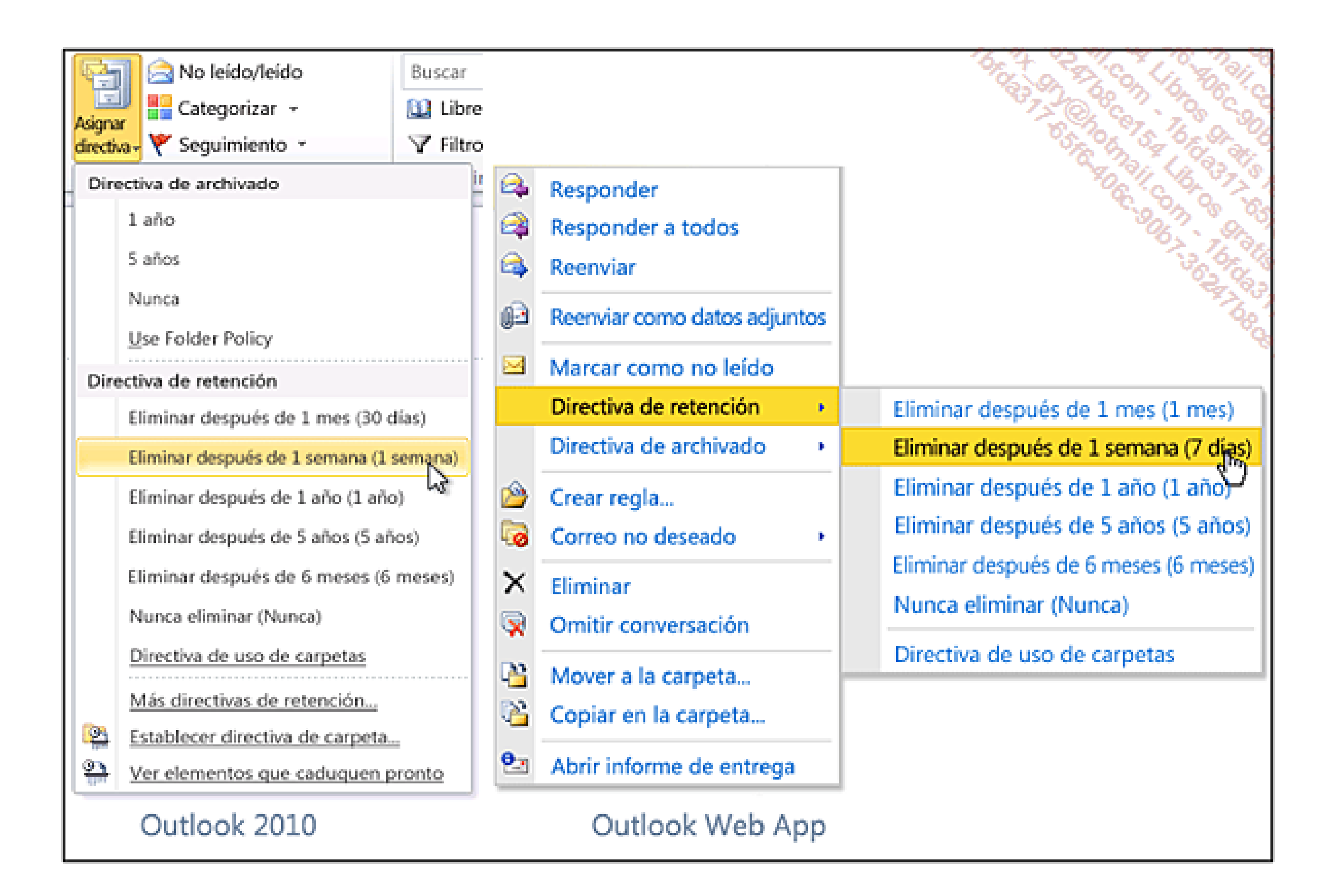
El archivado permite utilizar soportes más económicos para almacenar archivos más antiguos que solo tienen que estar disponibles de forma excepcional, quedando así asegurados.

Directiva de retención de documentos

En lo relativo a la retención de información, las empresas deben ser capaces de satisfacer las demandas de organismos profesionales y administrativos y, por tanto, de aplicar directivas de retención para los documentos.

Más allá de los documentos en papel, que incluyen firmas, hay cada vez más documentos completamente digitales que se deben conservar.

Es el caso, por ejemplo, de los correos electrónicos. Los entornos de correo más modernos (por ejemplo Outlook 2010 y Exchange 2010) admiten este tipo de opciones para permitir una retención gestionada a nivel de sistema:



Directiva de retención de Outlook 2010

b. Los servicios de gestión electrónica de documentos

Los documentos informáticos contienen información semiestructurada, es decir, sin organización predefinida, pero cuyo contenido puede ser tratado electrónicamente (búsqueda de palabras clave...). Pueden proceder perfectamente de documentos en papel escaneados y convertirse en un archivo (o no).

Tras los servicios de archivos, las aplicaciones de gestión electrónica de documentos (GED) permiten un tratamiento de la información bajo esta forma específica. La organización es más precisa que el simple esquema de árbol de archivos y la explotación es más cercana a la información contenida. La noción de archivos y su manejo se vuelve transparente para el usuario.

Gracias a los servicios de GED, el dato informático, en forma de textos, sonidos, vídeos, imágenes, gráficos, etc., es accesible a través de la red. Puede utilizar la red para circular a través de flujos previstos por procedimientos (*workflow*).

El término Gestión Electrónica de la Información y Documentos Existentes (GEIDE) es un complemento que designa la recuperación de los archivos de empresa en formato electrónico. Estos datos digitalizados se gestionan mediante esta aplicación. El escaneo de la información en formato papel es frecuente y las herramientas se han hecho muy eficientes (reconocimiento de texto, fotografías, mapas...).

c. Los servicios de base de datos

Las bases de datos permiten la utilización de datos electrónicos en forma estructurada. Su objetivo es doble:

- Facilitar la introducción de datos en un esquema predefinido (por ejemplo, en los campos de un formulario).
- Permitir su tratamiento de manera óptima, clasificados desde su introducción.

El almacenamiento de los datos se efectúa generalmente en bases de datos centralizadas. Existen aplicaciones dedicadas que permiten el acceso y la explotación de los datos (estadísticas, búsquedas...).

Se pueden encontrar varias familias de Sistemas de Gestión de Bases de Datos (SGBD). Por ejemplo, la gestión de los sistemas de archivos a menudo se realiza mediante este servicio. Los directorios informáticos residen en una base de datos, optimizada para la lectura. El lenguaje estándar para efectuar consultas de lectura y escritura en estas bases es LDAP (*Lightweight Directory Access Protocol*).

El trabajo con datos en forma de tablas, que pueden ser dependientes unas de otras, es lo propio de los Sistemas de Gestión de Bases de Datos Relacionales (SGBDR), o *Relational DataBase Management System* (RDMS). La programación de consultas estándar se realiza aquí en el lenguaje SQL (*Structured Query Language*).

d. Los servicios de impresión

Estos servicios de red permiten controlar y administrar dispositivos de impresión (como impresoras o faxes).

Su objetivo es compartir estos dispositivos exclusivos, con el fin de permitir una gestión coherente de las solicitudes de trabajos de impresión, integrando al mismo tiempo normas de prioridad que tienen en cuenta los formatos específicos de edición.

La implementación de una cola de impresión permite disminuir el número global de dispositivos de impresión, garantizando, al mismo tiempo, un acceso competitivo para los dispositivos. Internamente, los trabajos enviados a la cola de impresión se almacenan en un disco como archivos temporales.

Algunos dispositivos como los plóters (trazador gráfico) A0 en color son costosos. El hecho de compartirlos permite rentabilizarlos.

Poco a poco se va integrando el servicio de fax en la red de la empresa, lo que permite enviar y recibir documentos muy fácilmente. Esto implica una reducción considerable del tiempo de espera para el envío de un fax gracias a la gestión de una cola de envío. Se evita imprimir el documento, cuestión indispensable sin este servicio. De hecho, el documento se dirige hacia una impresora ficticia (el fax) y bajo forma electrónica hacia el fax del destinatario.

Hoy en día, muchas grandes empresas han emprendido proyectos para modernizar los medios de impresión con objeto de reducir los costes al máximo: nos encontramos muy a menudo impresoras multifunción o *Multi Function Printer* (MFP) que cumplen las funciones de impresora, fotocopiadora, fax y escaneo a correo electrónico (es decir digitalización del documento y posterior envío a la dirección de correo especificada).



Ejemplo de impresora multifunción de «grandes volúmenes»

e. Los servicios de mensajería y de trabajo colaborativo

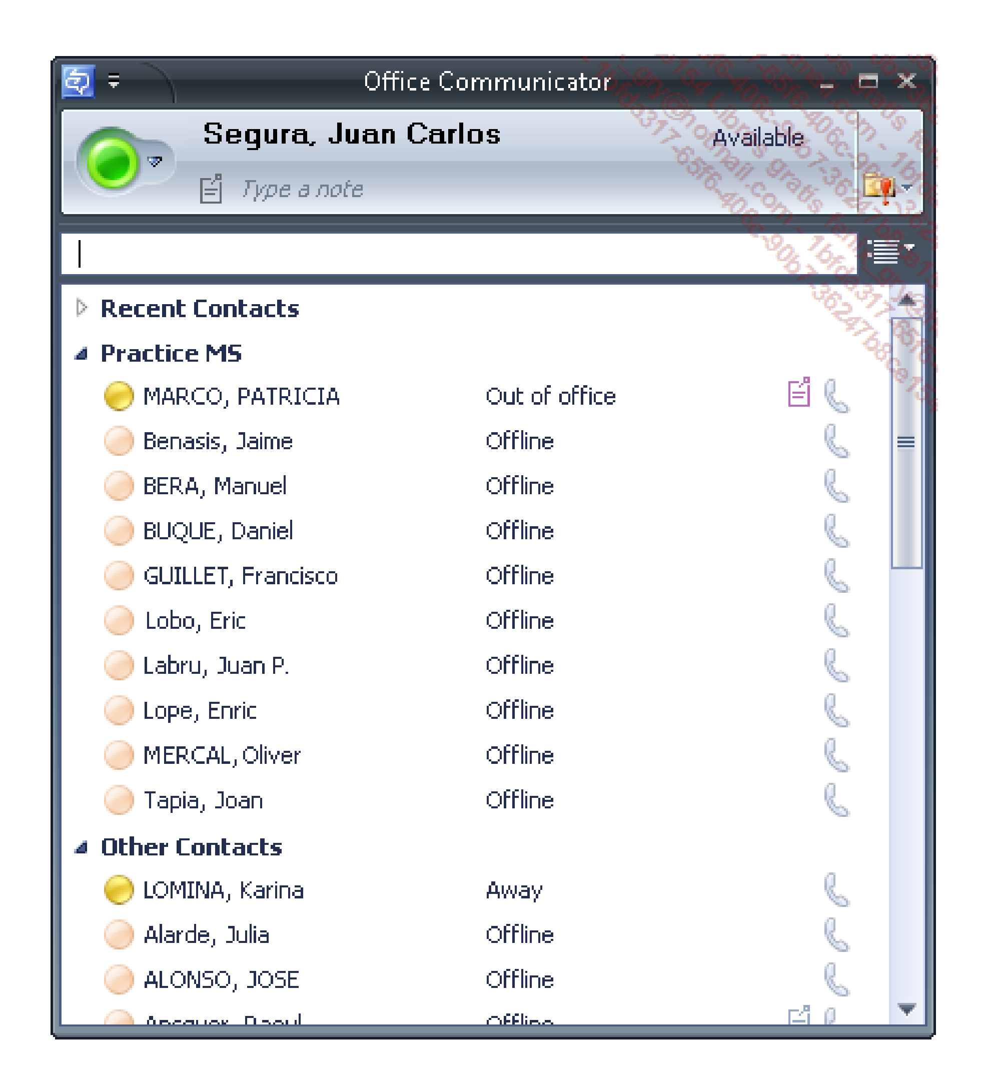
El servicio de mensajería electrónica agrupa el almacenamiento, la utilización y el envío de datos, incluidos los de tipo multimedia. Administra la comunicación asíncrona entre los usuarios o sus aplicaciones e informa de la llegada de un mensaje.

En los últimos años se ha optimizado con el servicio de mensajería unificado, capaz de administrar también faxes y servicios de contestador de voz.

El *groupware*, derivado de la expresión inglesa *group processes/software tools*, se traduce como trabajo colaborativo. Estos servicios añaden, a los de mensajería, herramientas para facilitar el trabajo entre varios usuarios, a través de agendas compartidas, tareas o notas, foros de discusión...

Las aplicaciones evolucionadas de videoconferencias, así como los sistemas de servicios de mensajería instantánea, son las últimas aportaciones a las funcionalidades existentes de trabajo colaborativo (*groupware*).

Nuevas funcionalidades, como la Presencia, permiten simplificar la colaboración con otras personas. El protocolo SIP (*Session Initiation Protocol*) permite soportar esta funcionalidad. Es muy fácil saber si una persona está disponible, ocupada, en una reunión, si ha salido, pero también es sencillo obtener la información que habrá dejado en caso de ausencia:



Ejemplo de utilización del cliente Office Communicator

f. Los servicios de aplicaciones

Permiten no solo compartir datos, sino también los recursos de tratamiento. El objetivo principal es la especialización de los servidores interconectados para distribuir lo mejor posible las tareas entre las máquinas adecuadas.

Supongamos que establecemos una conexión como clientes a un servidor que contiene un programa ejecutable y que solicitamos la ejecución de este programa. En el caso de un servidor de archivos, el archivo asociado a este programa será transferido a través de la red, se cargará en la memoria RAM del cliente y luego se ejecutará en el cliente.

En el caso de un servidor de aplicaciones, se establecerá una comunicación de igual a igual, en forma de mensajes entre el cliente y el servidor (petición del cliente que espera una respuesta del servidor). El cliente pide la ejecución de un programa que se encuentra en el servidor (hace la petición); el programa se ejecuta en el servidor y el resultado se devuelve al cliente (la respuesta). De esta forma, es el procesador del servidor el que trabaja para el cliente. Por eso un servidor de aplicaciones requiere, sobre todo, muchos recursos de ejecución (una máquina monoprocesador potente o incluso un multiprocesador); por el contrario, un servidor de archivos requiere mucha memoria RAM (utilizada como intercambio) para transferir los datos.

Desde hace algunos años, se habla mucho de SaaS o *Software as a Service* (aplicación como un servicio). Este concepto, que apareció en empresas como Citrix, ofrece un enfoque de aplicaciones bajo demanda.

En lugar de adquirir la licencia de un software o toda la infraestructura que permita gestionar un entorno, las empresas prefieren pagar por la solución de acuerdo con el uso que hacen de ella: la infraestructura se puede externalizar y alquilar las licencias de software en función de las necesidades. Puede tratarse de un software muy específico y costoso o incluso de aplicaciones

ofimáticas en línea.



g. Los servicios de almacenamiento

Las empresas gestionan cada vez más cantidades de datos (archivos, documentos y datos). El almacenamiento de los datos y su puesta a disposición de los usuarios se ha convertido en un problema en sí mismo.

Han aparecido, por tanto, nuevas soluciones que permiten realmente dedicar espacios de almacenamiento eficientes y capaces. Aunque al principio resultaban un poco costosos, estos sistemas han sabido evolucionar y actualmente resultan también interesantes para empresas pequeñas.

Network Attached Storage (NAS)



Servidor NAS

Un servidor NAS se integra en la red existente de una empresa, igual que el resto de los servidores (aplicaciones, base de datos...). Presta servicios comparables a los de un servidor de archivos, pero generalmente se mantiene dedicado.

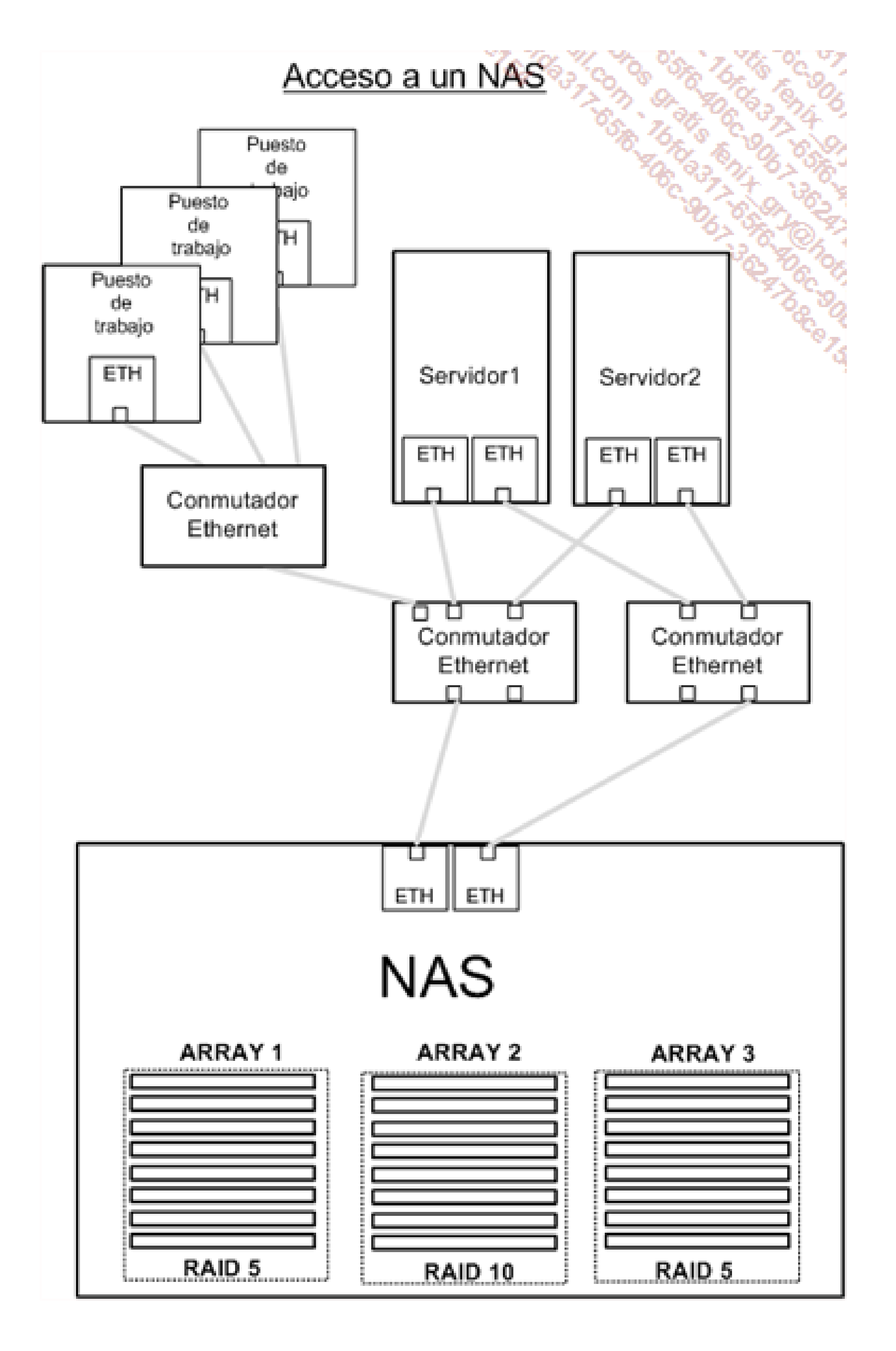
Principalmente se encontrará acceso a los servicios de archivos de Microsoft (CIFS o *Common Internet File System*), UNIX (NFS o *Network File System*) y HTTP (*Hypertext Transfer Protocol*). A

menudo también es posible compartir a través de FTP (*File Transfer Protocol*) y de AFP (*Apple File Protocol*), como se muestra a continuación.



Configuración de un NAS

De esta manera, no hay necesidad de un procesador potente ni de mucha memoria. En contraposición, ocupa un espacio de almacenamiento acorde, apoyado por soluciones de tipo RAID, de las que hablaremos más adelante.



Su sistema operativo puede ser específico, como propone Microsoft con Windows Storage. Al administrar varios protocolos de comunicación, un servidor NAS asegura el acceso a los recursos y también el acceso a través de la red, independientemente del tipo de cliente.

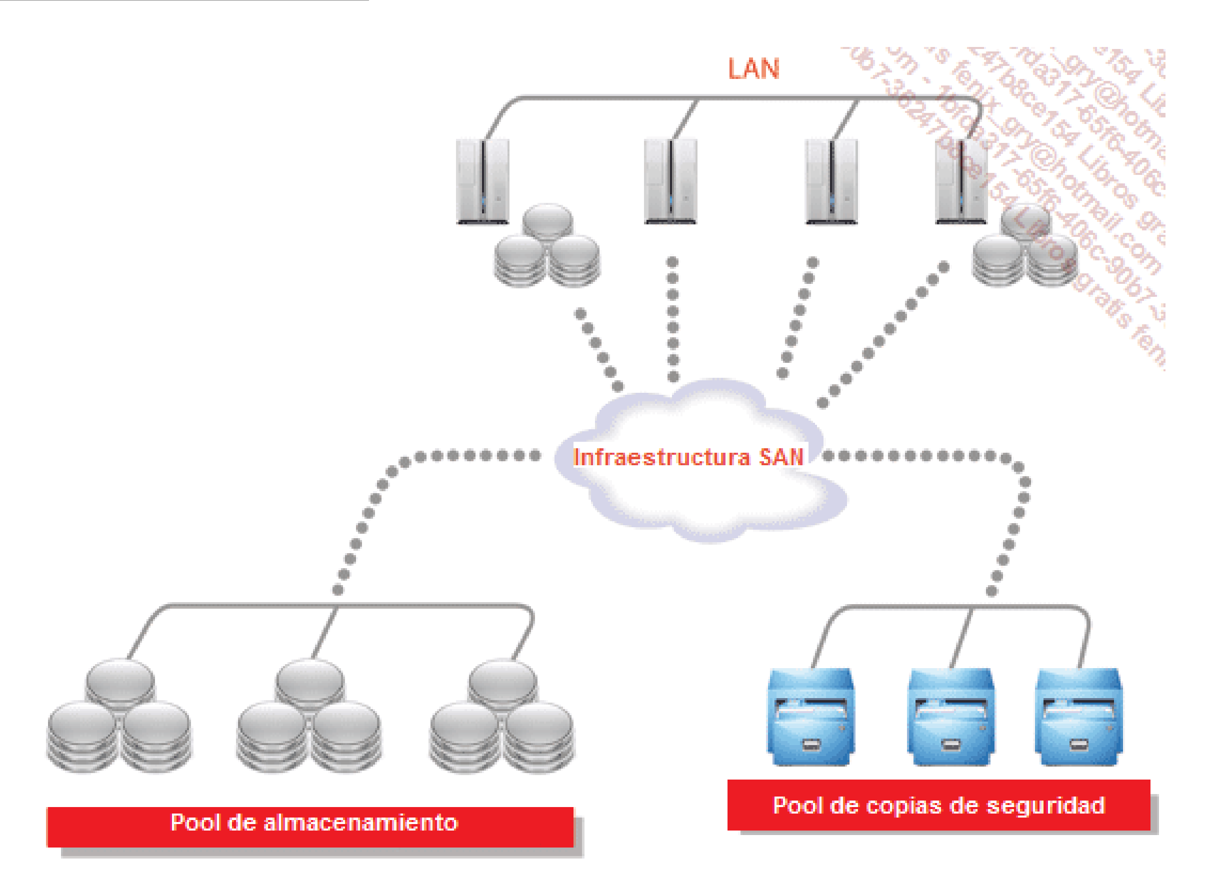
Esta tecnología presenta diferentes ventajas:

- Coste de compra inferior a un servidor de archivos tradicional.
- Aumento de la seguridad de los datos gracias a las redundancias físicas asociadas.
- Simplicidad de instalación y reducción del tiempo de administración de los servidores.
- Servidor universal en una red heterogénea.

Por extensión, un servidor NAS puede servir de destino de copias de seguridad y sustituir a una unidad de cintas. Su conexión directa a la red de la empresa permite situarlo en un edificio alejado del resto de los servidores, asegurando así las copias de seguridad sin manipulación de medios extraíbles.

Otro posible uso de los servidores NAS puede ser la puesta en marcha de dos unidades en dos salas de informática distintas. Mediante sincronización permanente de sus datos, se asegura la redundancia de la información con un coste muy razonable. Si se avería uno de los servidores, los usuarios pueden seguir trabajando con los datos almacenados en el otro servidor que continúa operativo.

Storage Area Network (SAN)



En un sistema SAN, se crea una nueva red dedicada a los datos. Actúa como red secundaria y «alivia» a la red principal de la empresa. Además de un aumento sustancial de la capacidad de acceso, se mejora la seguridad de los datos.

Los propios servidores de archivos están vinculados a esta infraestructura SAN. Se interconectan con una o varias unidades de almacenamiento para formar un pool dedicado. También es posible conectar unidades de medios extraíbles e incluso servidores NAS (*pool* de copias de seguridad).

Las unidades de almacenamiento son bahías de discos que ofrecen capacidades considerables y, sobre todo, evolutivas. Así, es posible añadir, en uso, discos duros adicionales para aumentar el espacio. Tener diferentes redundancias de hardware (discos duros, alimentación, conexión...) complementadas a veces con dispositivos de alerta a través de Internet ofrece una garantía de acceso a los datos.

En cada bahía de discos, se puede dividir el espacio de almacenamiento disponible. De esta manera es posible dirigir cada espacio lógico (LUN - *Logical Unit Number*) hacia uno u otro servidor de archivos. Estos últimos verán este aporte de almacenamiento como una unidad de disco local.

La eficacia de acceso entre los *pools* y los servidores de archivos se ve mejorada por el hecho de disponer de una red dedicada. Por el contrario, las tecnologías de infraestructura SAN son un poco diferentes de la red «clásica».

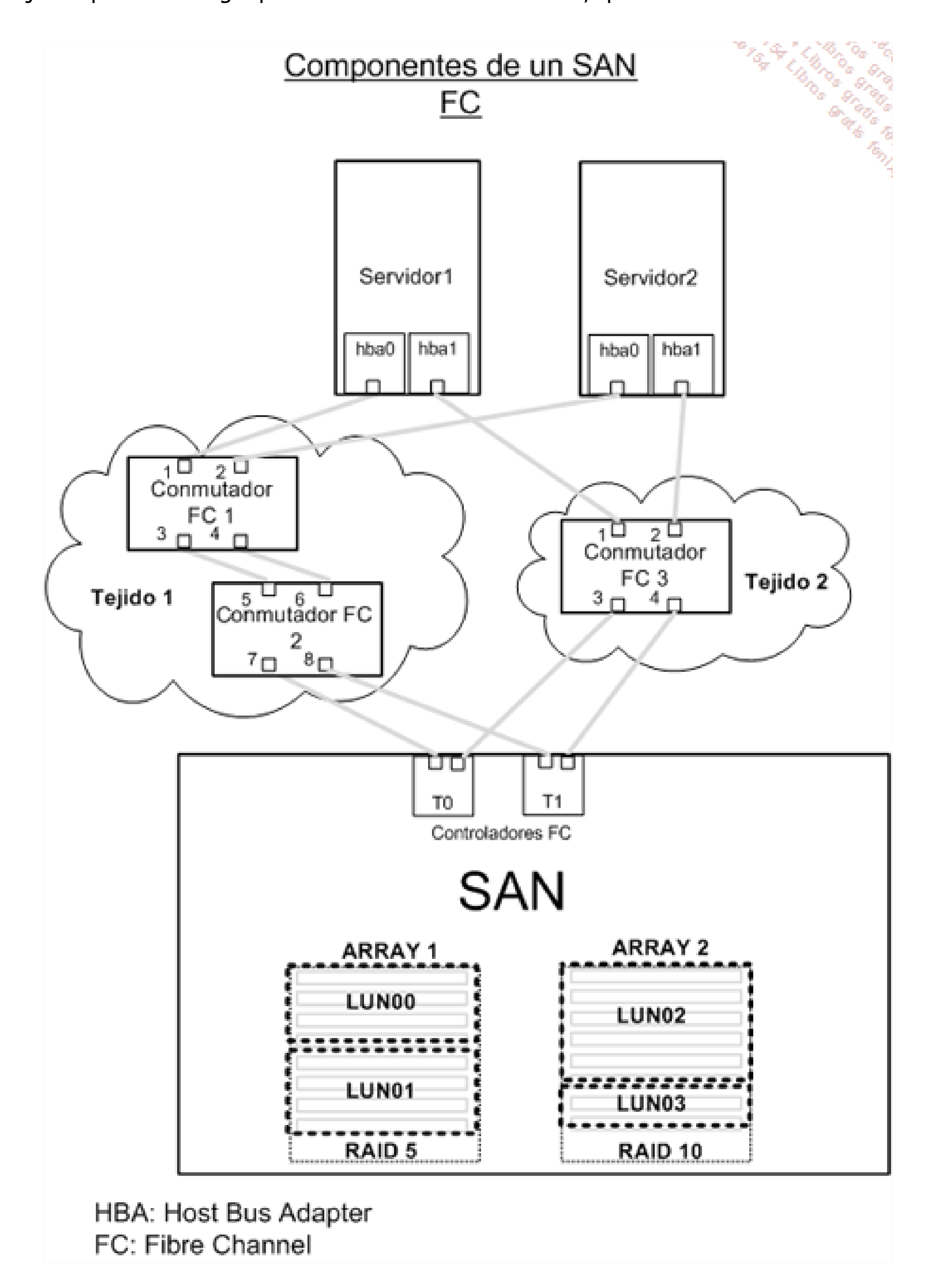
Durante mucho tiempo la red secundaria SAN estuvo compuesta por fibra óptica. Esta técnica, utilizada cuando la red es importante, permite flujos de hasta varios gigabits por segundo (normalmente entre 4 y 8 Gbps).

El SAN Fibre Channel (FC) está formado por un conjunto de elementos:

- Un sistema de almacenamiento, constituido por matrices de discos físicos (SATA o *Serial Advanced Technology Attachment*, SAS o *Serial-Attached SCSI*, SSD o *Solid State Drive*), divididos en volúmenes lógicos (LUN o *Logical Unit Number*).
- Controladores FC, que permiten restringir el acceso de una LUN concreta a una o varias conexiones de servidor. Cada conexión está definida por el *World Wide Name* de la tarjeta

HBA (*Host Bus Adapter*) del servidor.

- Tarjetas HBA que conectan el servidor a la red de dibra (Fibre Channel). Se utilizan como mínimo dos tarjetas para asegurar un mínimo de tolerancia a fallos.
- Conmutadores FC, que se utilizan para construir la red de interconexión y adjuntar la información de direccionamiento a los mensajes FC que se intercambian entre el origen y el destino.
- Los tejidos permiten agrupar diversos conmutadores, que se verán como uno solo.



Cada HBA (*Host Bus Adapter*) dispone de un nombre único o *World Wide Name* (WWN) (llamado también WWID), que es similar a una dirección MAC. El IEEE lo define en 8 bytes como un identificador único (*Organizationally Unique Identifier*).

Existen dos tipos de WWN:

- Para un **nodo** (*World Wide node Name* o WWnN), habitualmente una tarjeta HBA o un dispositivo SAN, que se puede compartir por algunos o por todos los puertos de un dispositivo (p. ej., una tarjeta HBA).

- Para un **puerto** (*World Wide port Name* o WWpN), que es obligatoriamente único para cada puerto (p.ej., cada puerto de una tarjeta HBA). Generalmente es el nombre que se mostrará para la conexión a un tejido SAN).

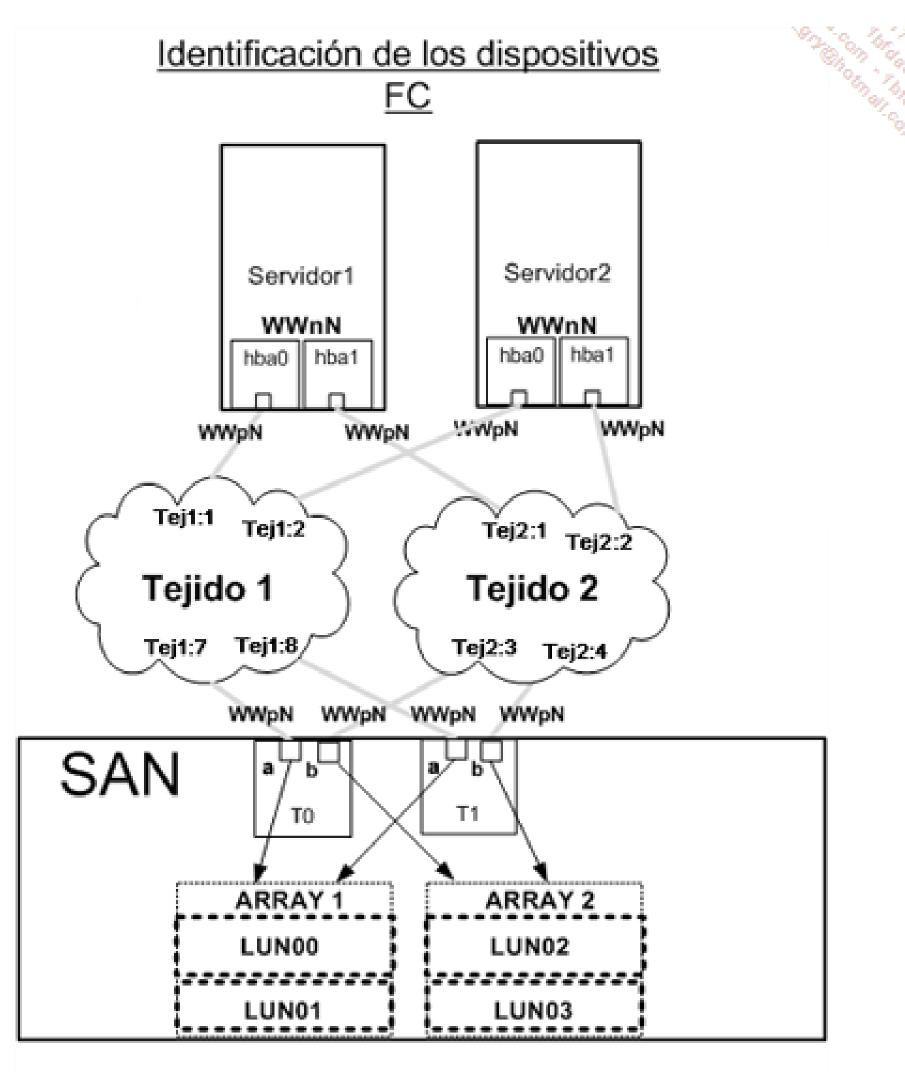
A continuación proporcionamos algunos ejemplos de WWN:

- 50:06:04:81:D6:F2:65:71 (subsistema disco EMC, el identificador EMC es '00:60:48', se ignora el primer carácter '5', y se cogen los seis caracteres siguientes).
- 10:00:00:00:c9:d8:e4:01 (tarjeta HBA Emulex, el identificador Emulex es '00:00:c9', se ignoran los cuatro primeros caracteres y se cogen los siguientes).
- 21:00:00:0e:8b:08:18:01 (tarjeta HBA Qlogic, el identificador Qlogic es '00:0e:8b').

El primer carácter hexadecimal (campo *Name Address Authority*) codificado en 4 bits permite identificar el modo en que se divide el WWN:

- '1', corresponde a «IEEE standard», que se descompone 10:00 + ii:ii:ii + hh:hh:hh.
- '2' corresponde a «IEEE extended», que se descompone 2 + h:hh + ii:ii:ii + hh:hh:hh.
- '5' corresponde a «IEEE Registered Name», que se descompone 5 + ii:ii:ii + h:hh:hh:hh:hh.

Donde h es el carácter hexadecimal codificado en 4 bits e i representa el identificador de la empresa (*Organizationally Unique Identifier*).



De este modo, las rutas de acceso disponibles a la bahía desde el servidor son:

Para el acceso a la bahía 1 (Array 1):

- Para el Servidor1, hba0 -> Tej1:1 -> Tej1:7 -> T0:a, o bien, hba0 ->Tej1:1 -> Tej1:8 -> T1:a

Para identificar las rutas potenciales, es más fácil empezar en la bahía y subir hasta el servidor en cuestión.

- Para el Servidor2, hba0 -> Tej1:2 -> Tej1:7 -> T0:a, o bien, hba0 -> Tej1:2, -> Tej1:8 -> T1:a

Para el acceso a la bahía 2 (Array 2):

- Para el Servidor1, hba1 -> Tej2:1 -> Tej2:4 -> T1:b, o bien, hba1 ->Tej:1 -> Tej2:4 -> T0:b
- Para el Servidor2, hba1 -> Tej2:2 -> Tej2:3 -> T0:b, o bien, hba1 ->Tej2:2 -> Tej2:4 -> T1:b

Existen muchas maneras de permitir el control de una LUN por un huésped. Se hablará de **zoning**para definir este acceso, enumerando todas las rutas disponibles entre un *initiator* y un *target*(destino). Un **zoning por software** que se realiza sobre un conmutador FC controla la visibilidad de las LUN basándose en los WWpN (en un lado el puerto HBA de un servidor, en el otro el puerto de la tarjeta controlador utilizada). Por su parte, el **zoning por hardware** se basa en los identificadores de los conmutadores (Domain ID), los números de los puertos implicados, en la entrada y la salida de un tejido.

iSCSI

Al contrario de la solución original basada en el protocolo FC que obliga a la utilización de equipos dedicados costosos (tarjetas HBA, conmutadores FC, etc.), se estandarizó en abril de 2004 (RFC 3720 y 3721) otra técnica más económica: iSCSI o Internet SCSI. El objetivo es hacer pasar comandos SCSI a través de una red TCP/IP. Se pueden utilizar el conector y los conmutadores Ethernet para construir esta red. Aunque menos eficaz que la solución FC basada únicamente en la fibra, con la llegada de Ethernet 10 Gbps las velocidades comienzan a ser muy interesantes.

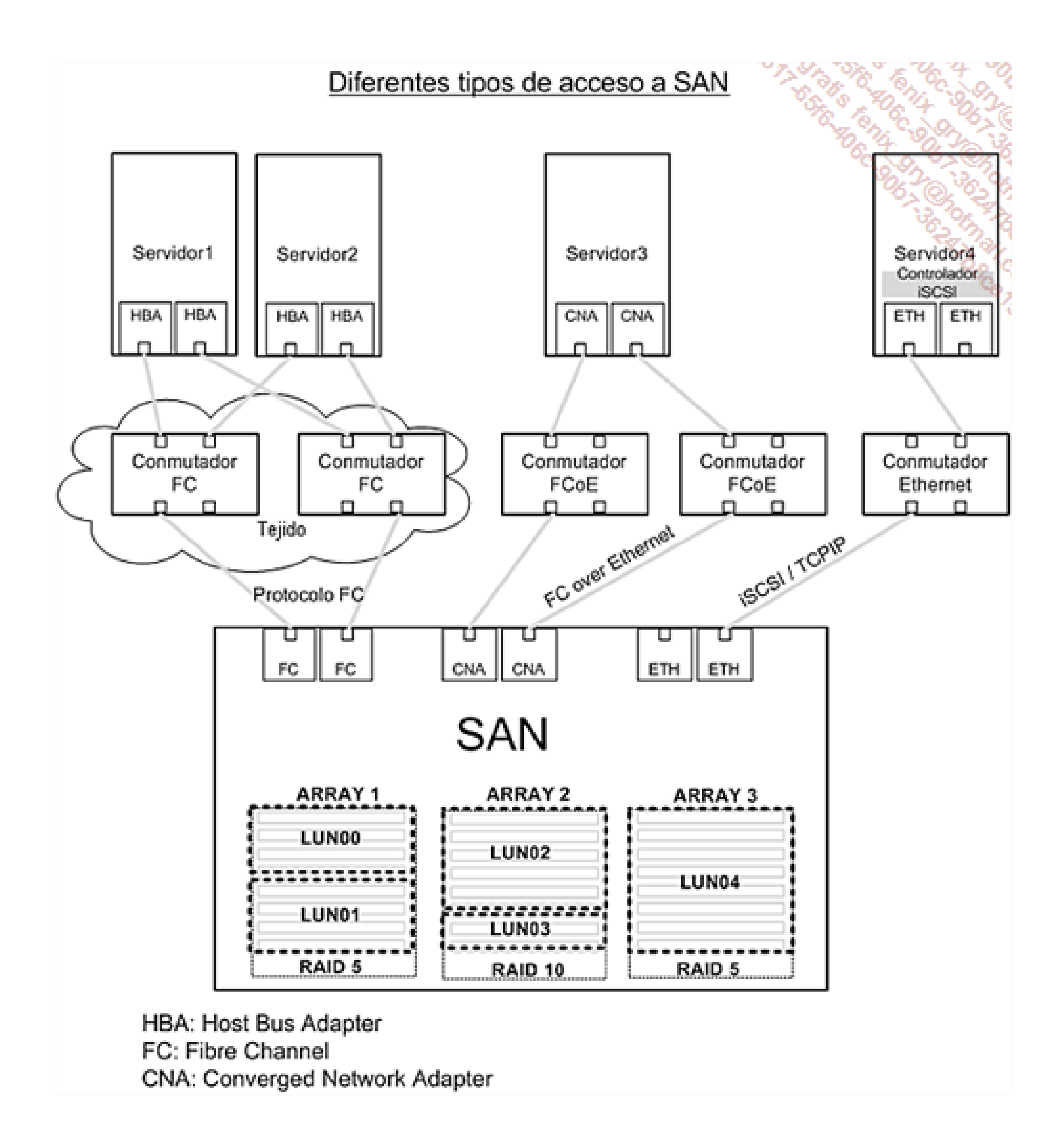
Por ejemplo, se encuentran soluciones de SAN iSCSI que ofrecen volúmenes modestos (1 a 16 TB) a precios razonables.



SAN iSCSI

FCoE o Fibre Channel over Ethernet

En junio de 2009, aparece FCoE. Su objetivo es posicionarse entre los dos mundos FC e iSCSI. FCoE ofrece una nueva clase de acceso Ethernet sin pérdida de paquetes (RFC 3643) con una encapsulación directa en Ethernet para optimizar la velocidad y tiene costes más bajos que la solución FC.



h. Los servicios de copia de seguridad

Deduplicación

La deduplicación de los datos es un mecanismo que tiene ya unos años, pero que comienza a hacer su aparición ahora en las empresas.

Evolución del volumen de datos

El volumen de datos generado por los sistemas de información no cesa de crecer a un ritmo desenfrenado. Se estima un crecimiento anual de entre un 30 y un 50 %. Estos elementos reflejan las novedades que aportan las principales herramientas ofimáticas que ahora almacenan sus datos de manera más óptima. Por ejemplo, la suite Microsoft, desde Office 2007, utiliza archivos XML y así optimiza el volumen de los archivos obtenidos. El simple hecho de pasar de una versión de Office 2003 a 2007 o 2010 permite generar, de media, documentos dos o tres veces más pequeños. A pesar de estas novedades, el volumen crece inexorablemente.

El aumento del volumen provoca que la duración de la creación de copias de seguridad sea cada vez más larga. Además, las aplicaciones cada vez son más críticas, lo que obliga a una reducción de las ventanas de copias de seguridad (rango horario autorizado para las ejecuciones de copias de seguridad).

Restricciones legales

Para dificultar más las cosas, las nuevas medidas legales exigen periodos de conservación de los

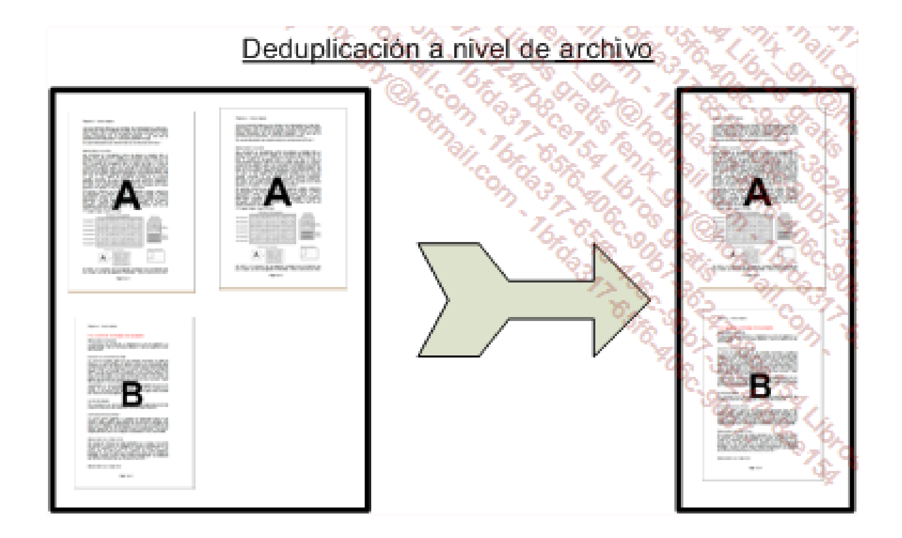
datos muy superiores a los actuales.

El SI cada vez más crítico

La criticidad también conlleva la necesidad de un reinicio rápido en caso de una incidencia grave, exigiendo mecanismos de restauración optimizados. Esto lleva a las empresas a ir progresivamente a almacenamientos en disco para la realización de las copias de seguridad, en lugar de soportes de tipo cinta magnética, con el fin de minimizar la duración de la restauración. Los soportes magnéticos han sido relegados a la externalización de los datos fuera de las instalaciones de las empresas.

Deduplicación a nivel de archivo

Se basa en eliminar archivos redundantes en un soporte. Por ejemplo, el sistema de correo electrónico de Microsoft (Exchange Server) utiliza este mecanismo para impedir la duplicación de archivos. De este modo, un e-mail enviado con un archivo adjunto a 50 usuarios de la misma organización Exchange solo adjuntará el archivo una única vez. Se habla de almacenamiento de instancia única o *Single Instance Storage* (SIS). Este mecanismo permite lograr tasas de reducción de 5 a 1.



Deduplicación a nivel de bloque

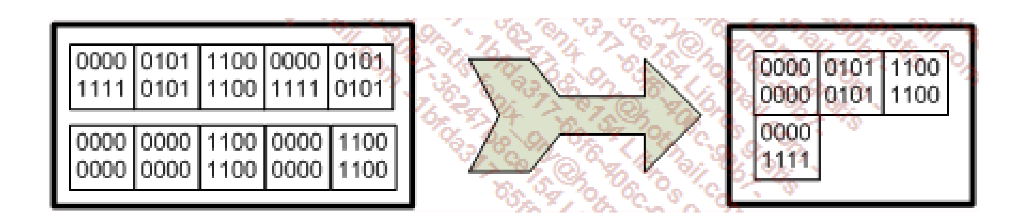
Otro enfoque mucho más eficaz es la deduplicación a nivel de bloque, es decir, a nivel de un segmento de archivo. De este modo, los mismos archivos de sistema estarán en todas las copias de seguridad completas que provengan de un mismo sistema operativo de máquinas diferentes. Es fácil comprender que la deduplicación será particularmente eficaz.

Este tipo de deduplicación puede lograr tasas de reducción de 20 a 1.



Deduplicación a nivel de byte

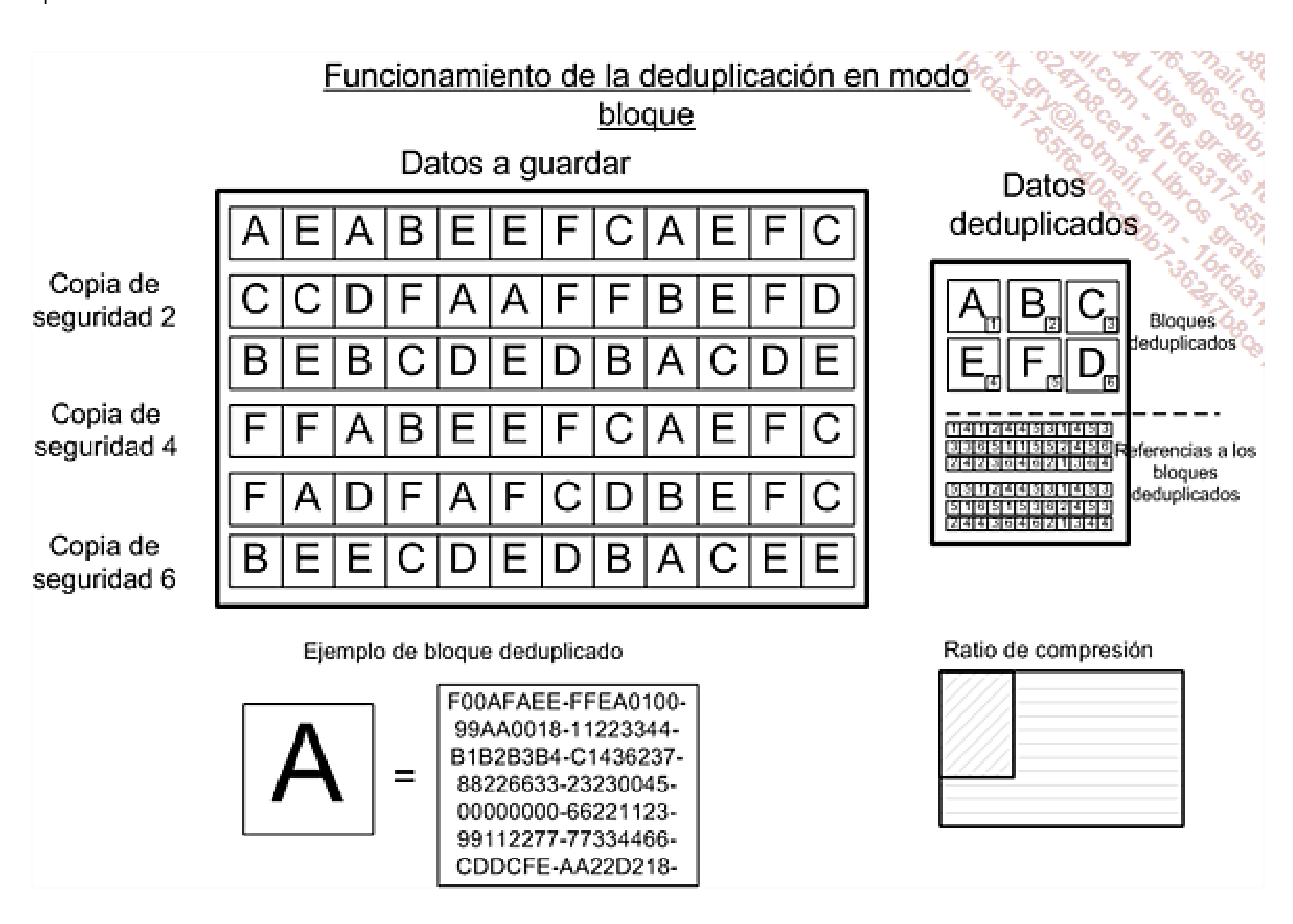
Existe una tercera técnica que se basa en los bytes.



Deduplicación en destino

Estas limitaciones han llevado a los fabricantes a ofrecer en un primer lugar soluciones basadas en la optimización de los datos una vez archivados, basándose en un mecanismo llamado**deduplicación en destino**. De hecho, el principio de copia de seguridad sigue siendo el mismo que en un modo de funcionamiento clásico, pero, una vez los datos están disponibles en el soporte principal de la copia, se analizan y optimizan identificando los bloques comunes presentes en el conjunto de los juegos de copias realizados. Estos bloques son de longitudes variables, generalmente entre 32 KB y 128 KB. De este modo, si realiza copias de seguridad completas de sus sistemas (datos incluidos) centrándose en sistemas operativos idénticos, la tasa de deduplicación será extremadamente elevada para la parte del sistema operativo (SO). Igualmente, los datos ofimáticos del mismo tipo que provengan de la misma aplicación van a generar una tasa de compresión más alta.

Por ejemplo, imaginemos que tenemos que realizar seis copias de seguridad. El algoritmo de deduplicación identificará los bloques comunes y ofrecerá la mejor descomposición posible para permitir una compresión elevada. Durante una deduplicación en destino, el algoritmo será capaz de identificar los mejores bloques de todos los que ya se han copiado. El soporte de la copia conservará el conjunto de bloques duplicados, así como los índices que hacen referencia a los bloques utilizados.



Del mismo modo, la multiplicación de las copias de seguridad completas no afectará más que a las copias diferenciales. Incluso si esta solución reduce considerablemente las necesidades en materia de volumen de archivado, las operaciones de copia siguen siendo las mismas.

Las soluciones basadas en VTL (*Virtual Tape Library*) utilizan generalmente este tipo de mecanismo reemplazando cintas por discos, en forma de cinta virtual. La gestión en modo disco permite

realizar posteriormente operaciones de deduplicación, que no se pueden realizar en cintas físicas.

Deduplicación en origen

Otros fabricantes han llevado sus ideas más lejos, ofreciendo una solución que tenga en cuenta la deduplicación desde el origen. La ventaja principal de este enfoque se basa en la no transmisión de la totalidad de los datos, aunque sí de los bloques deduplicados. Por otra parte, el algoritmo de deduplicación de bloques anticipa los bloques comunes incluso antes de tener todas las copias. La eficiencia es menor puesto que la base de referencia de los bloques es menos extensa.

Avamar (adquirido por EMC), Simpana (CommVault), Veeam Backup (VEEAM) ofrecen soluciones basadas en la deduplicación en origen.

i. Los protocolos de replicaciones entre bahías

En una configuración donde se busca la tolerancia a fallos, en la que se implementa una solución con dos servidores redundantes, naturalmente se va a tratar de garantizar la tolerancia a fallos en los datos asociados (bases de datos o datos asociados a un servicio). Para ello, cuando elegimos una solución de tipo NAS o SAN que integra componentes redundantes (alimentación, discos RAID, red redundante, controladores duplicados), se puede enriquecer la solución, ofreciendo una replicación de los datos sensibles en segundo plano a otra sala.

Para esto se utilizarán herramientas complementarias ofrecidas por los fabricantes de bahías informáticas, a través de licencias complementarias.

La solución completa, servidores redundantes (clústers) y datos replicados (GeoCluster de datos) permite disponer de una solución real con tolerancia a fallos y ofrecer una reanudación, con interrupción del servicio, pero sin pérdida de datos, según el modo de replicación implementado.

El primer modo **síncrono** asegura la sincronización de las actualizaciones casi simultáneas entre las bahías: cualquier actualización de la primera bahía se hace garantizando la misma actualización en la segunda. En caso de que haya algún problema, aparte del tiempo de reinicio, los datos replicados en la segunda sala son idénticos a los de la primera. El mayor inconveniente es que este modo exige tiempos de latencia entre salas extremadamente bajos, permitiendo solo conexiones de tipo Fibre Channel. Las distancias posibles se limitan a algunas decenas de kilómetros. En el caso de dos edificios situados en un mismo lugar, la solución es particularmente interesante.

El modo **asíncrono** permite una mayor flexibilidad en el funcionamiento con una desincronización posible y un tiempo de latencia más elevado. De este modo es posible basarse en una red IP existente y permitir distancias casi ilimitadas. Dado este retraso entre las actualizaciones en segundo plano, en caso de error, será necesario adaptar los datos para no tener en cuenta las operaciones que se han replicado en la segunda bahía. Este mecanismo de limpieza es admitido por los gestores de bases de datos que se utilizan, basándose en el diario de transacciones.

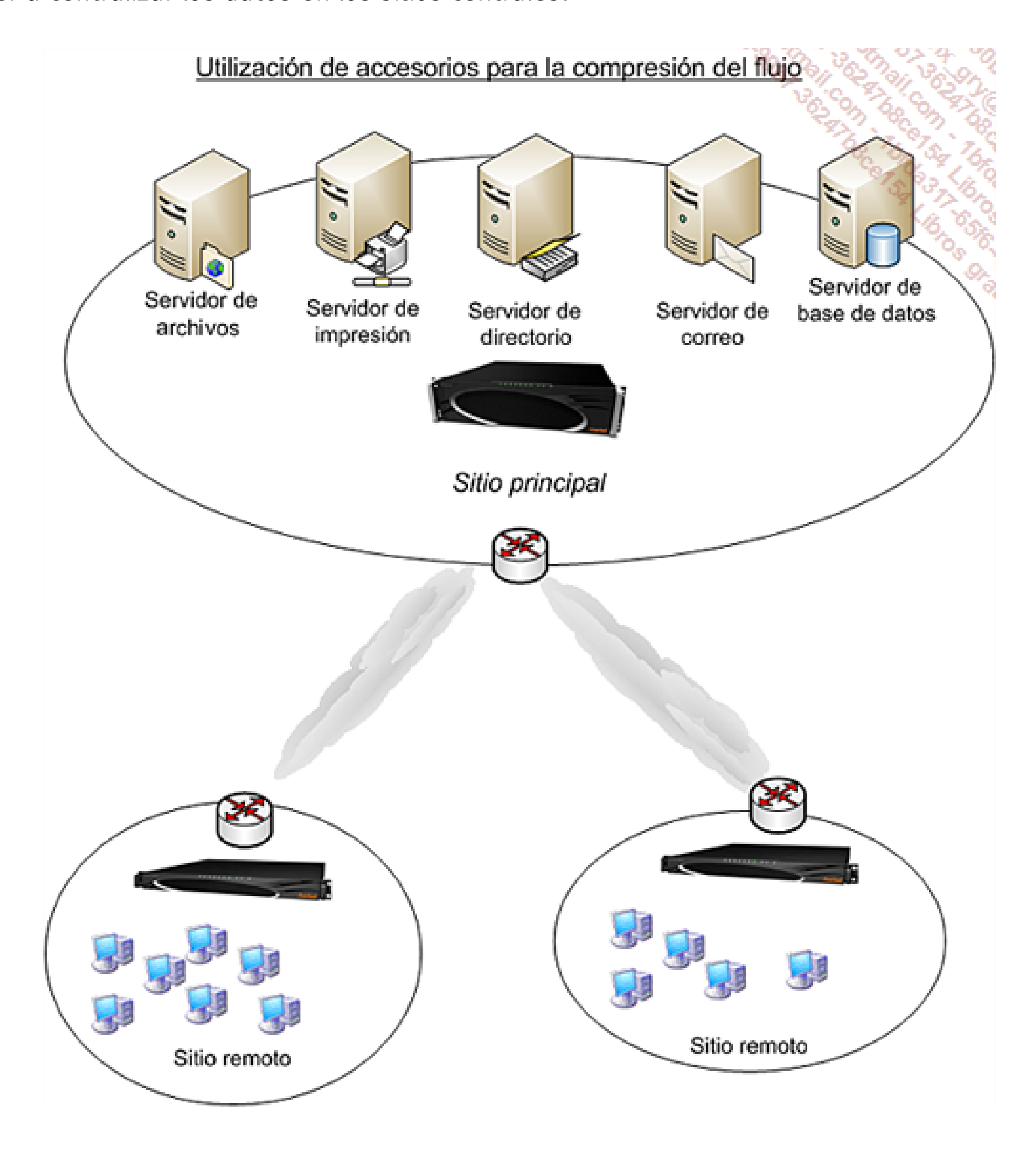
Ciertos programas de gestión de clúster pueden ofrecer funcionalidades de replicación entre bahías (p. ej., HACMP o *High Availability Cluster Multiprocessing* solution Cluster, ofrecido por IBM en un UNIX AIX).

Los principales productos de replicación entre bahías con los siguientes. Todos estos productos gestionan a la vez el modo de replicación síncrona y asíncrona:

- SRFD o *Symmetrix Remote Data Facility*, de EMC, permite la replicación y la restauración de bahías Symmetrix.
- PPRC o *Peer-to-Peer Remote Copy*, de IBM.
- Continuous Access EVA gestiona la replicación entre bahías EVA 3000 o 5000.
- True Copy Remote Replication de HDS (*Hitachi Data Systems*) asociado a ShadowImage permite hacer una replicación síncrona acoplada con dos replicaciones asíncronas en sitios remotos.

WAFS y compresión del flujo

Desde hace algunos años, las empresas que funcionan con sucursales tienen que hacer frente a dos visiones contradictorias: implementar una solución de almacenamiento local en sitios remotos o volver a centralizar los datos en los sitios centrales.



Teniendo en cuenta las interacciones entre los sitios centrales y los sitios distantes, los anchos de banda WAN limitados (incluso si la velocidad ha evolucionado considerablemente), la elección no siempre es sencilla. Una solución complementaria a la elección de datos centralizados es la utilización de dispositivos compresores de flujo.

Han aparecido soluciones dedicadas a los servicios de archivos y de impresión: los dispositivos WAFS (*Wide Area File Services*).

Los dispositivos WAFS han heredado las funcionalidades de los dispositivos de compresión de datos de los años 2000, así como de los equipamientos que tienen en cuenta la gestión de la prioridad (QoS o *Quality of Service*).

Estos dispositivos efectúan también la aceleración de numerosas aplicaciones basadas en la capa de transporte TCP administrando la caché para evitar transmisiones inútiles.

Esta solución ofrece numerosas ventajas:

- Compresión de los datos: se implementa una deduplicación de datos de aplicación que transitan en conexiones TCP o en intercambios UDP. Se analizan los datos a nivel de byte

para asegurar que solo los datos no redundantes se transmiten a través de la red.

- Transparencia: este tipo de soluciones permite simular servidores de archivos en sitios remotos de manera transparente para los usuarios y con poca latencia.
- Disponibilidad de las modificaciones: se puede acceder a los archivos localmente ayudándose de una caché y, cuando se realizan las modificaciones, solo se replican los nuevos cambios (a nivel de byte).
- Bloqueo de archivos: cuando un usuario abre un archivo para modificarlo, otro usuario que quiera acceder al mismo archivo desde otra ubicación solo lo podrá abrir en modo de solo lectura.
- Acceso a versiones anteriores: gracias a la utilización de *snapshots* (copias instantáneas) en el servidor principal, es posible tener acceso a las versiones anteriores de un archivo desde cualquier ubicación remota.
- Añadido en tiempo real: cuando un usuario añade un nuevo archivo desde una ubicación, es visible inmediatamente en todas las ubicaciones, incluso si el contenido se ha cargado posteriormente.
- Alta disponibilidad: cuando hay un problema en una infraestructura WAFS, se produce una resincronización para tener en cuenta todas las modificaciones que han tenido lugar a nivel de las diferentes cachés presentes en cada ubicación.

Los principales proveedores son Nortel, Brocade, Cisco, Packeteer y Riverbed.

4. Virtualización

a. Introducción

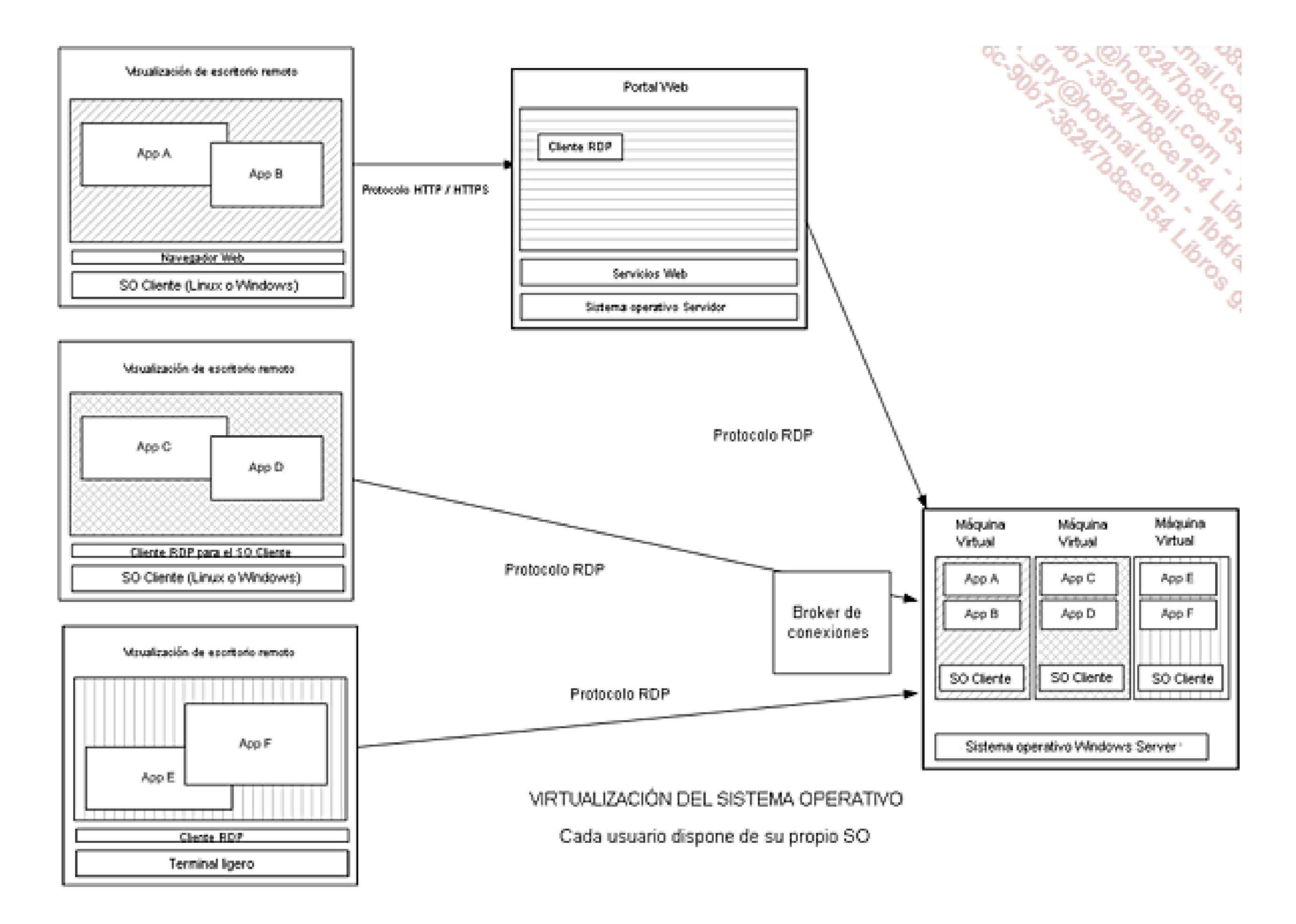
La búsqueda permanente de la disminución de costes con mejores niveles de servicios ha conducido de forma natural a la generalización de la virtualización de entornos. Una de las primeras cosas que condujo a la virtualización fue constatar que, en los servidores, los recursos están casi todo el tiempo infrautilizados (RAM, procesador, disco, red). Uno de los primeros objetivos es optimizar la utilización de estos recursos, ofreciendo, en los entornos virtuales más sofisticados, una asignación dinámica (a petición) de estos.

Ya presente desde los años 70 con los MainFrame, la virtualización forma parte integrante de las arquitecturas x86.

b. Algunos conceptos de virtualización

Los primeros entornos de virtualización se centraron en sistemas operativos de servidor. Actualmente, se han generalizado soluciones de virtualización para puestos de trabajo: se habla de VDI o *Virtual Desktop Infrastructure* (término introducido inicialmente por VMWare). Se encuentran también soluciones centradas en la **virtualización de aplicaciones**.

En general, si se trata de un entorno de puesto de trabajo o servidor, se habla de **virtualización de sistema operativo**.

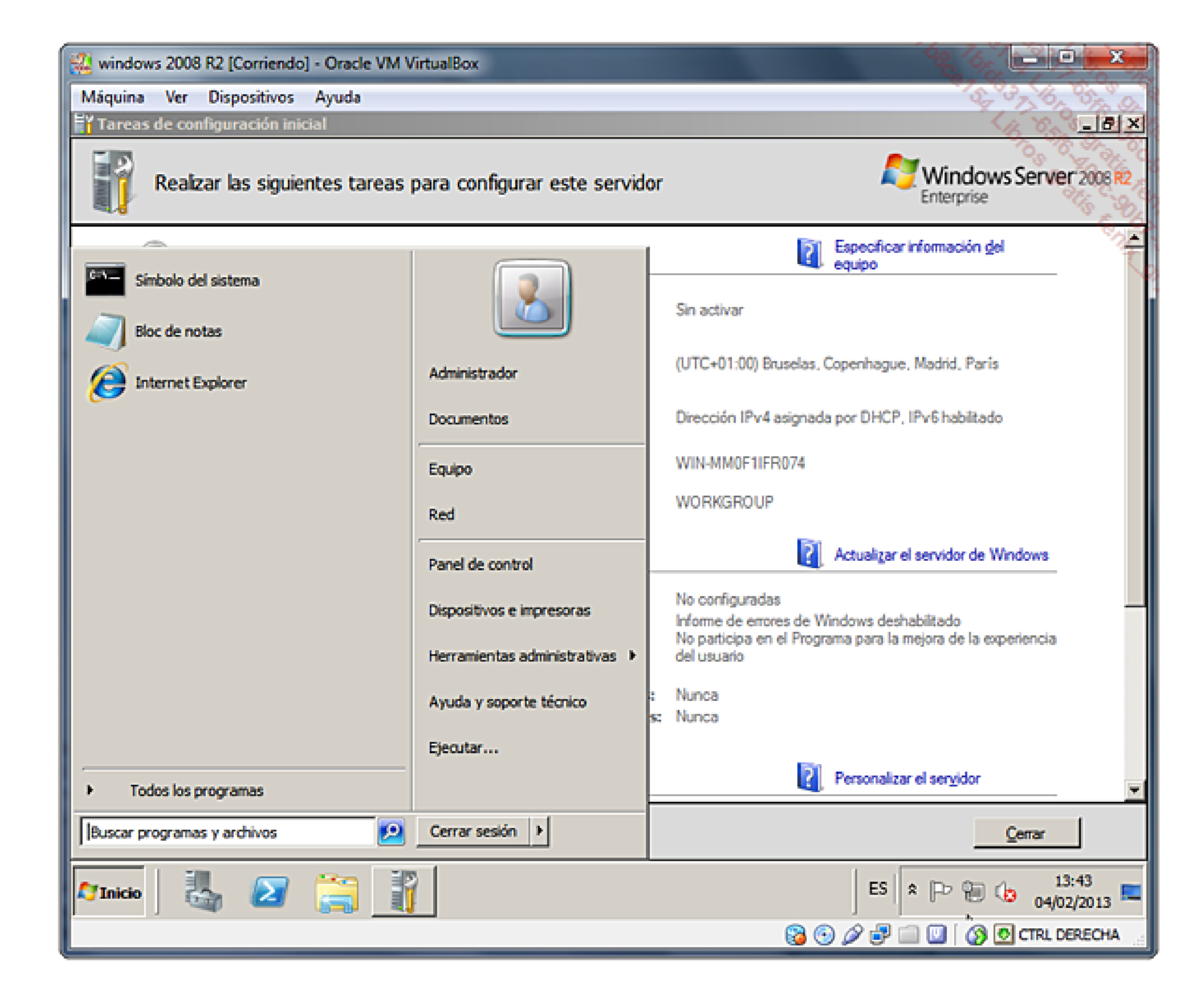


El acceso a los puestos de trabajo virtualizados pasa por un **Load Balancer** (balanceador de carga) también llamado **Broker de sesiones**.

Los principales proveedores en este ámbito son VMWare VIEW, que se ayuda de vSphere, Citrix XenServer o incluso Microsoft Hyper-V.

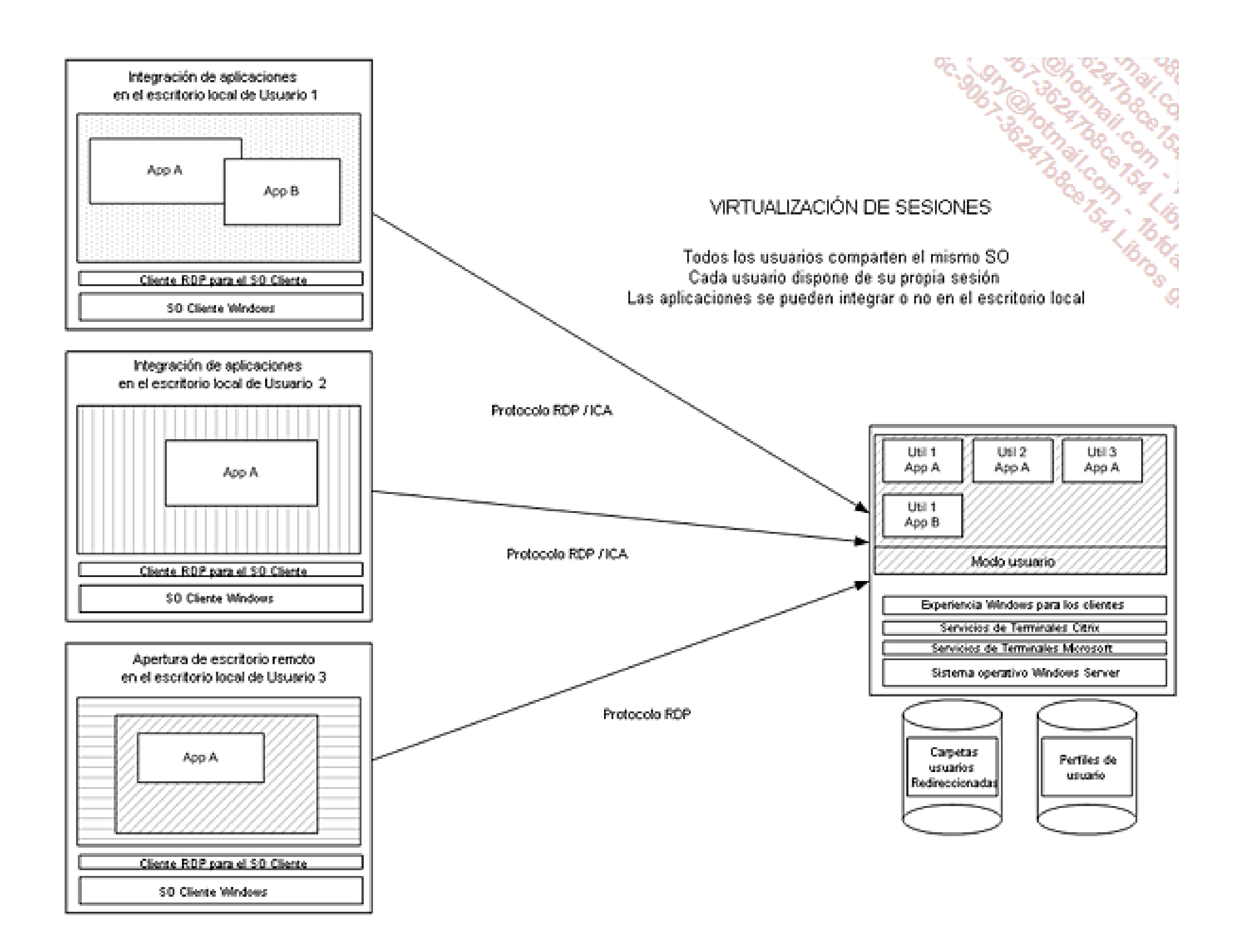
Existen también versiones gratuitas para emular un entorno virtual en un puesto de trabajo (modo maqueta): Sun VirtualBox, Microsoft Virtual PC o incluso VMware Server.

En este modo, la principal diferencia con VDI es que la emulación del SO se hace en el mismo equipo.



Ejemplo de un SO servidor virtualizado en un puesto de trabajo

El término **virtualización de sesión** se utiliza igualmente para hacer frente a la ejecución de aplicaciones en servidores en modo presentación: la aplicación se ejecuta en un servidor remoto y se visualiza en el puesto de trabajo apareciendo completamente integrada en el escritorio del usuario.



La **virtualización de aplicaciones** significa una solución en que la aplicación se empaqueta en un entorno aislado y se pone a disposición en los puestos de trabajo, generalmente, vía*streaming*. Esta aplicación no está instalada en el equipo pero se ejecuta correctamente en él.

En el mercado hay disponibles diferentes soluciones, como VMware ThinApp, Microsoft App-V, Symantec Endpoint Virtualization Suite (antes Altiris SVS) o Citrix XenApp.

Plan de continuidad de la actividad

Las empresas utilizan la informática para almacenar datos que pueden contener información confidencial. Por ello, es importante garantizar su protección tanto durante el almacenamiento como en la entrega de datos.

La disponibilidad permite garantizar el servicio en cualquier circunstancia y para ello se requiere la implementación de soluciones que hagan más fiables los servicios y los medios de almacenamiento.

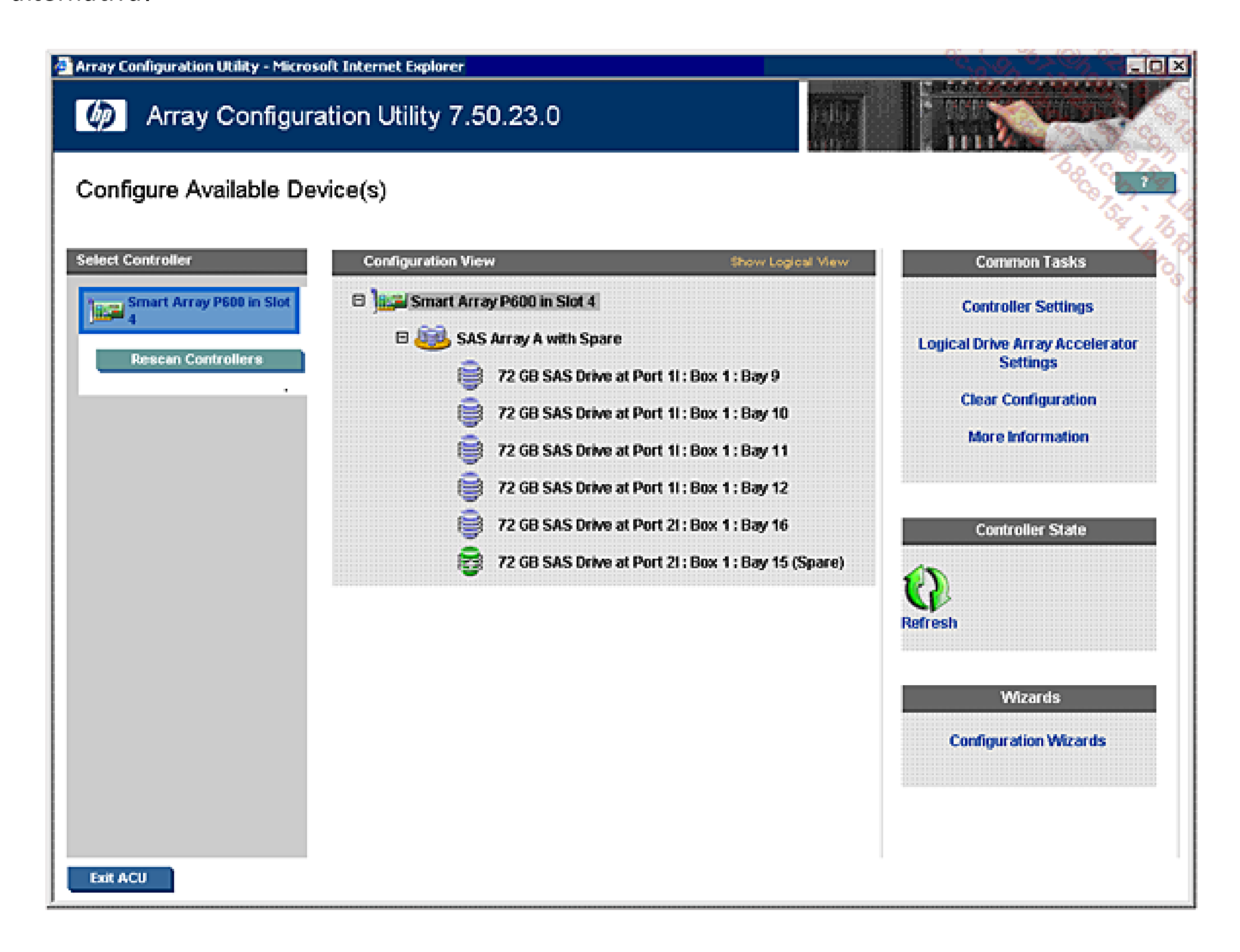
Los principios de confidencialidad también son importantes, ya que protegen la visibilidad de los datos. Los cálculos de integridad permiten, por su parte, prevenir pérdidas de información. Sobre estos conceptos volveremos más tarde en el capítulo Principios de protección de una red.

1. Disponibilidad

a. La fiabilización del sistema de almacenamiento

Redundancia de los datos

Es posible implementar una redundancia de medios para garantizar una buena tolerancia a fallos a través de la duplicación de datos en dos o más discos duros. Algunas soluciones *Redundant Array of Inexpensive Disks* (RAID), o conjunto redundante de discos independientes, permiten esta alternativa.



Utilidad de configuración HP

Protección eléctrica

A veces, también es necesario proteger eléctricamente las máquinas imprescindibles de una red (servidores, equipos de conexión...) contra las subidas de tensión o los cortes eléctricos. Con este fin, los Sistemas de Alimentación Ininterrumpida (SAI) o (UPS - *Uninterruptible Power Supply*) actúan como filtro de tensión. Permiten también compensar la alimentación principal del hardware conmutando la fuente de alimentación con una batería.



Sistema de alimentación ininterrumpida

Sistema transaccional de archivos

Este sistema de transacción se establece explícitamente en el sistema de archivos (en el caso de Novell Netware), o implícitamente como en el caso de Linux (Ext4) y Windows (NTFS).

Igualmente se puede hablar de JFS (*Journaled File System*), disponible en IBM AIX o ZFS (*Z File System*), de Sun Solaris.

Integridad de datos y CRC

Los sistemas de archivos ejecutan un mecanismo de cálculo de integridad de los datos almacenados, a través de códigos de redundancia cíclicos (CRC - *Cyclic Redundancy Check*).

El inicio de un cálculo de CRC es un polinomio generador, cuyo valor binario es conocido, por ejemplo los 17 bits 10001000000100001 para un CRC de 16 bits. Se efectúa un cálculo a partir de este polinomio y de los bits que deben comprobarse. Cuando se repiten las mismas operaciones, el resultado se compara con el anterior para comprobar que no hay error. El sistema está diseñado para detectar tanto los errores repartidos aleatoriamente como los secuenciales, de longitud inferior al tamaño del polinomio. La mayoría de los tramos de errores superiores o iguales al polinomio también pueden identificarse.

b. La fiabilización de los intercambios

Soporte físico fiable

Una manera sencilla de garantizar una fiabilidad en el intercambio de información es utilizar un soporte de transmisión fiable, por ejemplo la fibra óptica, insensible a cualquier perturbación electromagnética.

Puntos de sincronización

En el intercambio de información crucial, como la que permite la actualización de bases de datos, es necesario poder efectuar una recuperación del contexto antes del incidente, estableciendo estas protecciones de contexto o puntos de sincronización.

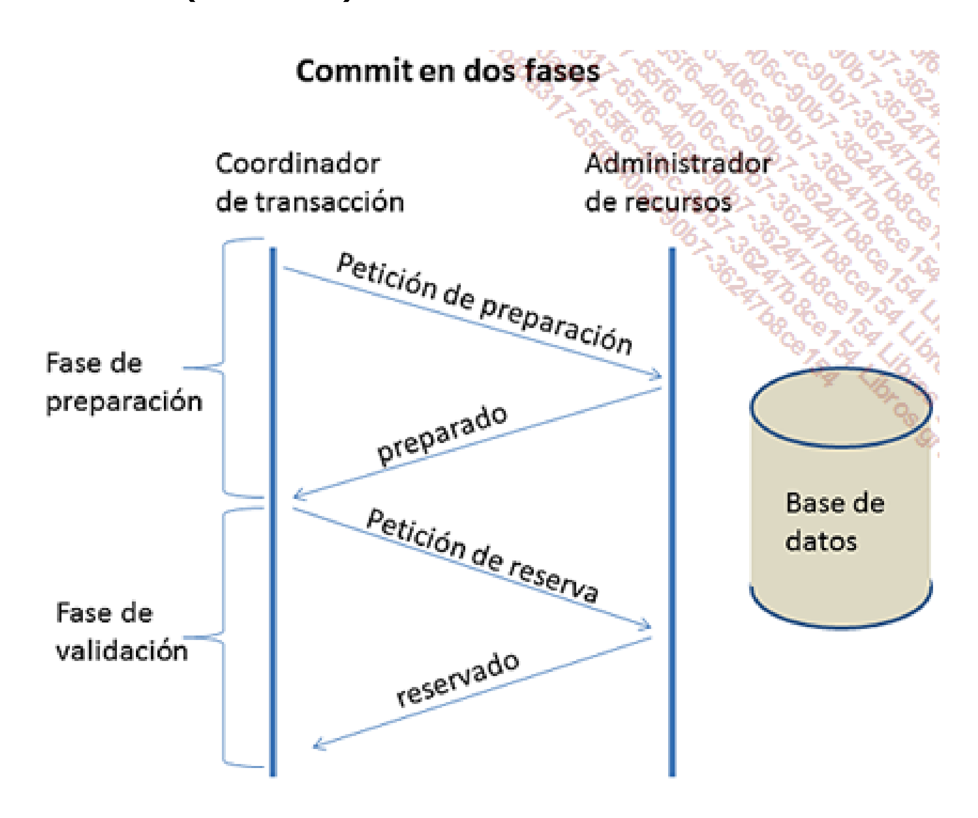
Guardando periódicamente las modificaciones, es posible recuperar el contexto inmediatamente anterior al incidente. De hecho, es importante saber exactamente cuáles fueron las modificaciones que se tuvieron en cuenta durante la última transacción anterior al incidente.

Protocolos en modo conectado

Los protocolos conectados aseguran fiabilidad en los intercambios gracias a los acuses de recibo y a los códigos de redundancia cíclicos.

Transacciones a nivel de aplicación

Cuando, por ejemplo, se realizan actualizaciones importantes en bases de datos, es esencial hacer operaciones unitarias, incluso si hay problemas. Para esto, uno de los mecanismos más conocidos es el **«commit» (validación) de dos fases**.



2. Confidencialidad

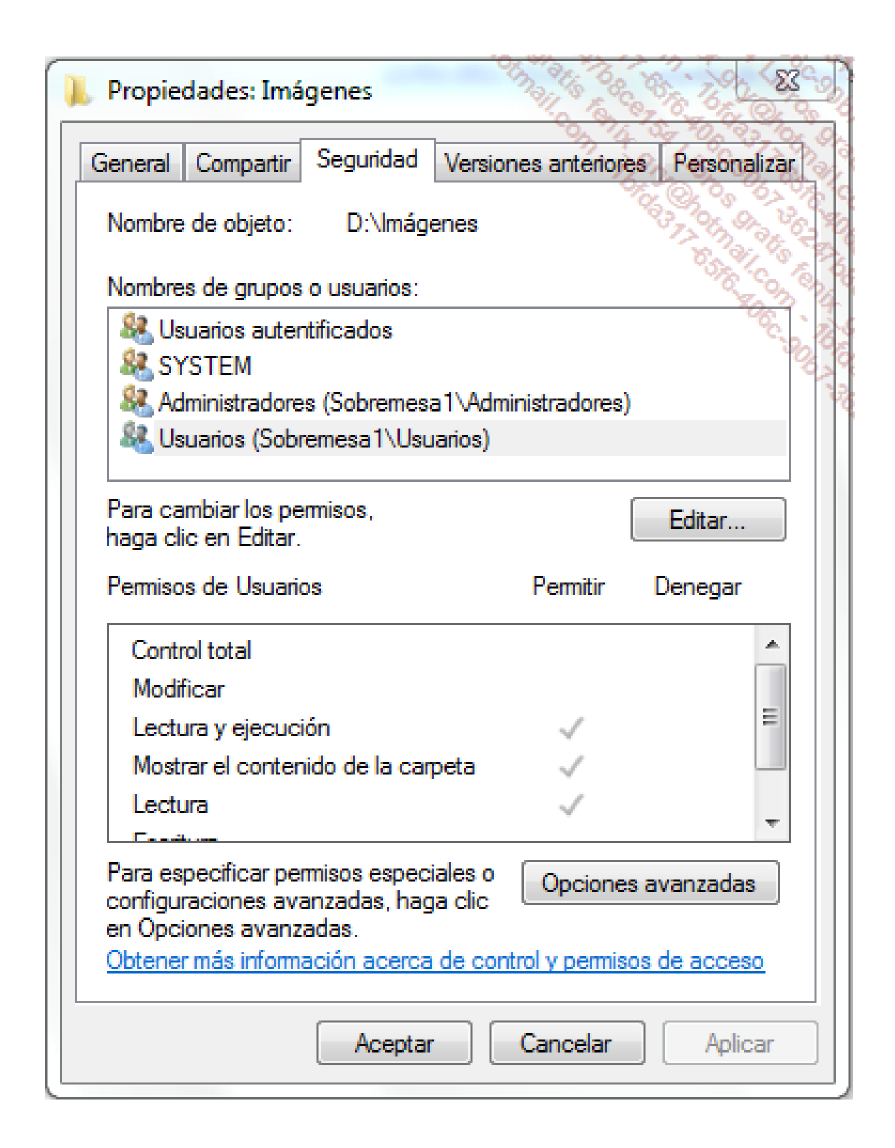
a. La seguridad del sistema de archivos

La primera solución para garantizar la confidencialidad de los datos puede ser aportada por el sistema de archivos que utiliza el sistema operativo.

Para poner en marcha la seguridad local, es necesario poder identificar cada acceso.

Para poder identificar, ante todo es necesario autentificar los usuarios. Por ello, en un sistema de archivos seguro, es necesario basarse en la autentificación inicial.

Un sistema de archivos seguro tiene en cuenta a los usuarios del sistema para administrar reglas de seguridad personalizadas a nivel de los archivos.



Administración de permisos locales en Windows

Por ejemplo: los sistemas Windows ofrecen NTFS (*New Technology File System*). Linux utiliza el sistema de archivos Ext4, que muestra los permisos elementales (RWX) para tres tipos de usuario (el usuario propietario, el grupo propietario y el resto). Los sistemas operativos Unix utilizan sistemas de archivos diferentes pero que emplean los mismos conjuntos de permisos.

b. La protección de los intercambios

Autentificar

El establecimiento de una conexión a menudo está precedido por una autentificación que valida el acceso a los recursos remotos.

De hecho, todos podemos marcar un número de teléfono para conectarnos con un módem remoto o introducir la dirección de un servidor público. Para ello es necesario validar el acceso a la red en primer término y después el acceso a la información.

El cifrado

La confidencialidad de la información es necesaria a menudo durante la transmisión de datos en distintos y variados soportes. De hecho, tomando como principio que es imposible impedir a alguien interceptar las tramas en una red y que resulta incluso menos posible saber si nuestras tramas han sido leídas, es preferible procurar que la información transmitida no sea legible para cualquiera.

Para convertir esta información en confidencial, se debe codificar mediante un cifrado, también llamado encriptado. De esta manera solo el emisor y el receptor pueden leerlo.

Las herramientas de análisis de tramas permiten la lectura y la interpretación de los flujos que circulan si no están cifrados. Microsoft proporciona, con las versiones de servidor de sus sistemas operativos, un programa de este tipo, el monitor de red, en una versión limitada.

Igualmente podemos encontrar herramientas gratuitas, WireShark y TCPDump, disponibles para varios sistemas operativos y que pueden descargarse de Internet.

Los sitios web www.wireshark.org y www.tcpdump.org permiten obtener información sobre estas herramientas, así como acceder a su descarga.

Internet y confidencialidad

Un dato confidencial que viaja por Internet, como el número de una tarjeta de crédito, puede ser interceptado por personas mal intencionadas si este no está encriptado.

Por ello recurrimos al cifrado de la información confidencial (nombre y contraseñas) o incluso de la totalidad de los datos.

También la legislación al respecto ha evolucionado en España. Los métodos de cifrado pueden superar los 128 bits en ciertas condiciones.

3. Redundancia de datos

a. La tolerancia a fallos

La tolerancia a fallos se puede definir como una configuración de hardware o software que permite prevenir uno o más tipos de averías susceptibles de perjudicar el buen funcionamiento del sistema, de retrasar o afectar un proceso o un usuario.

Para los discos duros, aunque existen soluciones de software, se utiliza especialmente la tolerancia a fallos por hardware. Esta permite la sustitución en caliente (*hot plug*), es decir, sin apagar el ordenador. Entre las soluciones que ofrecen tolerancia a fallos, encontramos:

- RAID 1, o espejo (*mirroring*), en el cual las operaciones de lectura y escritura tienen lugar simultáneamente en dos discos.
- RAID 2, otro dispositivo de espejo que no necesita un segundo disco en las operaciones de lectura (obsoleta).
- RAID 3, bloques de intervalo con paridad hacia un disco dedicado.
- RAID 5, bloques de intervalo con paridad distribuida conectados a un ensamblaje de discos.
- RAID 5 + 1, combinación de bloques de intervalo con paridad, puestos en espejo.
- RAID 0 + 1, combinación de *stripping* (bloques de intervalo) y espejo...

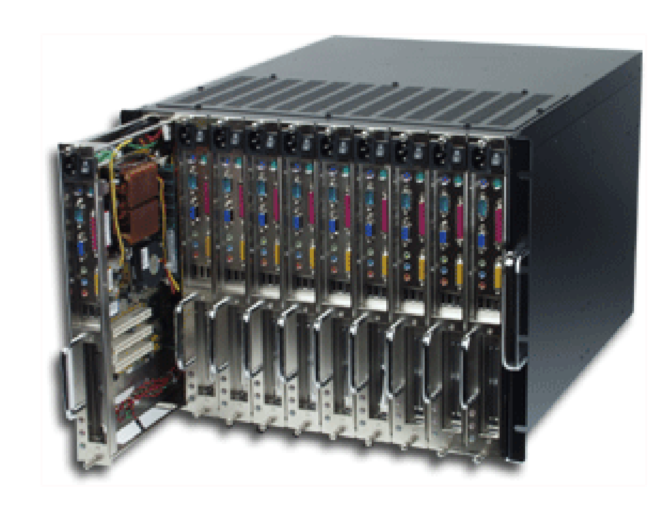
Ninguna de las soluciones RAID incluye la tolerancia a fallos. Por ello, el modo RAID 0, calificado de bloques de intervalo (stripping) sirve principalmente para acelerar las operaciones de escritura, ya que distribuye los datos entre varios discos y de manera transparente para el usuario.

Dentro de un servidor, los componentes como la alimentación y los ventiladores también disponen de mecanismos de tolerancia a fallos.



Servidor 2U con alimentación redundante

Los tradicionales, completos y autónomos servidores en forma de torre se han visto reemplazados hoy día por versiones integrables en estantes (*racks*). Su tamaño es más pequeño debido a que se han quitado algunos componentes. Se les llama servidores pizza, aunque incorporan discos duros o placas (*blade*), tarjetas muy simples que integran un mínimo de componentes.



Placas en chasis

De esta manera, resulta mucho más sencillo duplicar los servidores e implementar mecanismos de tolerancia a fallos a este nivel. Los datos puede traspasarse entre dispositivos llamados bahías de discos, que también se colocan en *racks*.

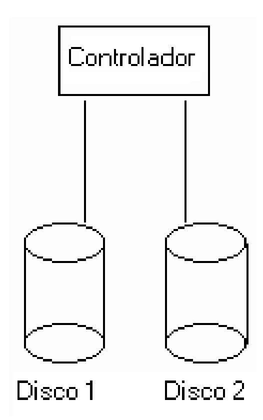


Sistema de almacenamiento de discos IBM

b. El espejo de discos

En el modo espejo, se conectan dos o más discos duros al mismo bus de datos. Los bloques de datos grabados en el disco primario también se graban en el disco secundario.

Los discos funcionan en tándem. Graban y actualizan los mismos archivos. En caso de fallo de uno de los discos, el otro continúa funcionando ininterrumpidamente y sin pérdida de datos.



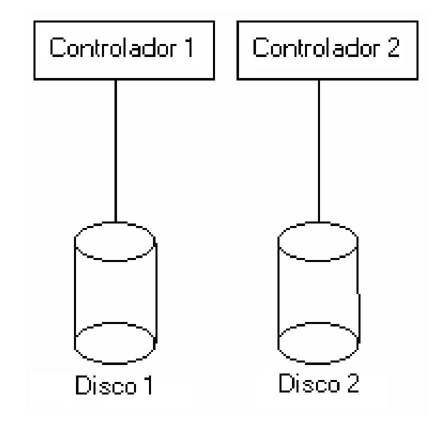
El modo espejo no es suficiente para garantizar la protección de los datos. De hecho, si los dos discos duros sufren una avería al mismo tiempo, o si el propio ordenador presenta algún defecto, se pierden los datos. Contra esto, se recomienda hacer copias de seguridad regularmente.

En caso de fallo de uno de los discos, el sistema operativo envía un mensaje para reportar el incidente y para que la protección en modo espejo se restablezca cuanto antes. Como este modo duplica los datos de los discos que se encuentran conectados al mismo bus de datos, no puede garantizar la protección entre los discos duros y el servidor en caso de avería del bus de datos. Un incidente de este tipo implicará un fallo de los dos discos a la vez.

c. El espejo de controladores y discos

Este método de duplicación de datos permite garantizar la protección de los datos. Consiste en copiar los datos en dos discos distintos, utilizando dos buses de datos distintos.

Así se protegen los datos en caso de fallo de un disco duro o del bus de datos que conecta el disco duro con el servidor (este bus de datos incluye la controladora de discos y el cable de interfaz). Si uno de los elementos de un bus de datos está defectuoso, el otro disco sigue funcionando, ininterrumpidamente y sin pérdida de datos, puesto que se transmiten por otro bus de datos. En este caso, el sistema operativo enviará un mensaje de advertencia para indicar que una unidad está defectuosa.



Tampoco basta con el modo duplicado para garantizar la protección de los datos. De hecho, si los dos buses de datos de los discos sufren una avería en el mismo momento o si el propio ordenador presenta algún defecto, se pierden los datos. En este caso, también se recomienda hacer copias de seguridad regularmente.

En modo duplicado los mismos datos se registran simultáneamente en todos los discos. Para los discos que están conectados a buses diferentes, la transferencia de datos es mucho más rápida

que en el modo espejo, donde los datos se transmiten sucesivamente hacia los discos y a través del mismo bus de datos.

Este modo también posibilita las búsquedas distribuidas que envían solicitudes de lectura hacia varios discos y esperan una respuesta más rápida. Si varias solicitudes llegan al mismo tiempo, se distribuyen entre los discos duplicados y, en consecuencia, son tratadas simultáneamente.

d. Bloques de intervalo con paridad

Bloques de intervalo

El modo de escritura en bloques de intervalo (*stripping*) ejecuta simultáneamente varios discos con el fin de acelerar los procesos. Además de no permitir la tolerancia a fallos, disminuye el tiempo de lectura.

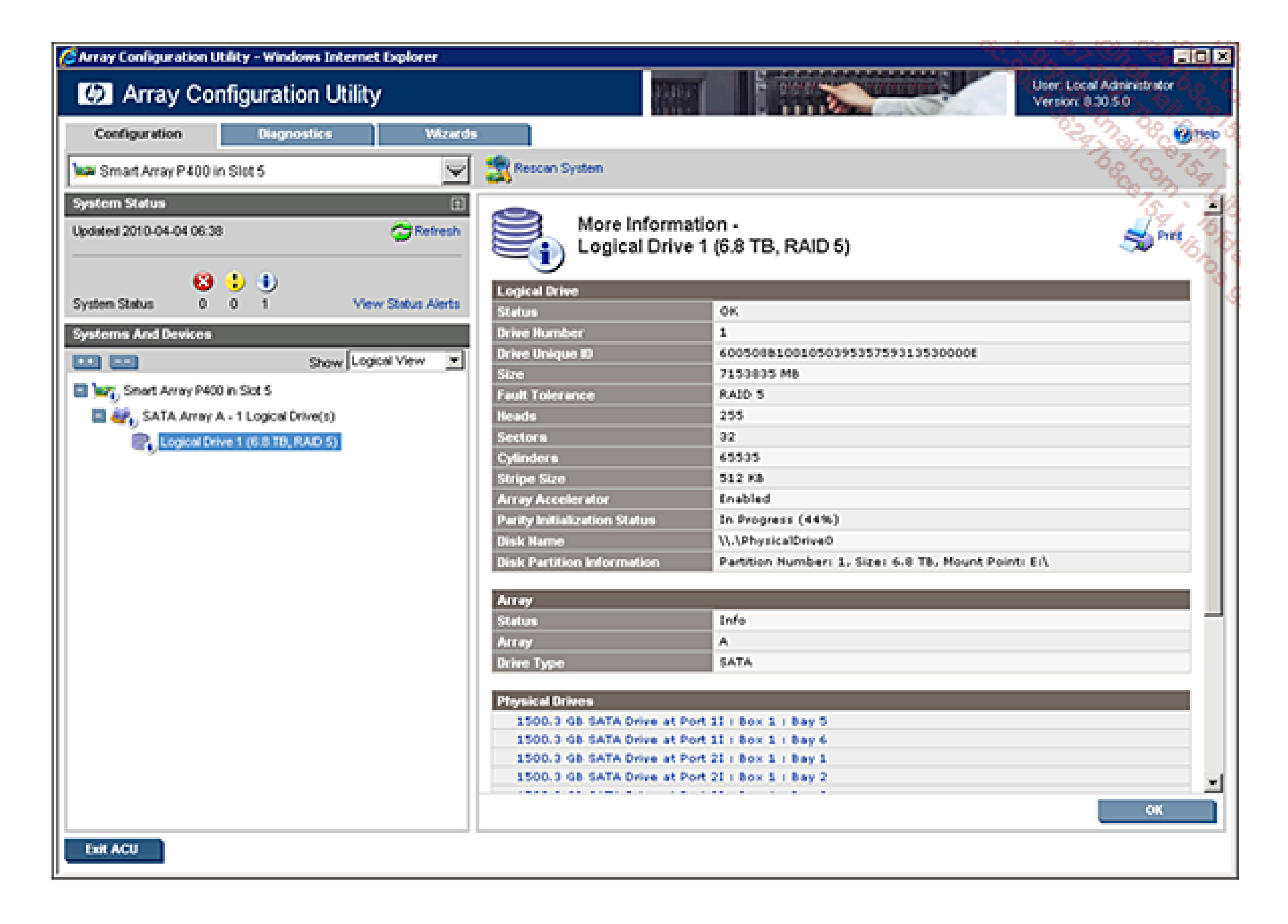
Cada uno de los soportes está dividido en bloques pequeños de igual tamaño. La escritura de un archivo podrá abarcar una serie de bloques repartidos en varios discos duros.

El bloque de intervalos está estandarizado con el nombre RAID 0.

RAID 3, RAID 5 y RAID 6

Los bloques de intervalo con paridad representan el sistema más utilizado para concebir una estrategia de tolerancia a fallos de disco.

RAID 3 es una solución en la que la paridad se almacena en un disco dedicado. Con RAID 5, la información de paridad se distribuye en un disco diferente en cada intervalo.



Configuración RAID 5

La técnica RAID 6 es una evolución de RAID 5. Las soluciones 3 y 5 solo permiten un fallo de disco en la serie. Si se produce el fallo en dos unidades, se pierden los datos almacenados y hay que restaurarlos. Aquí, las operaciones de paridad se duplican y se vuelven más complejas, lo que

permite el fallo conjunto de dos discos duros sin incidencia para el usuario. Con la disminución de costes, esta solución, que no es nueva, se utiliza cada vez más.

Paridad

Además de escribirse en el bloque de intervalos, la información de paridad se registra en un disco con el fin de recuperar los datos en caso de fallo de uno de ellos, cualquiera que sea.

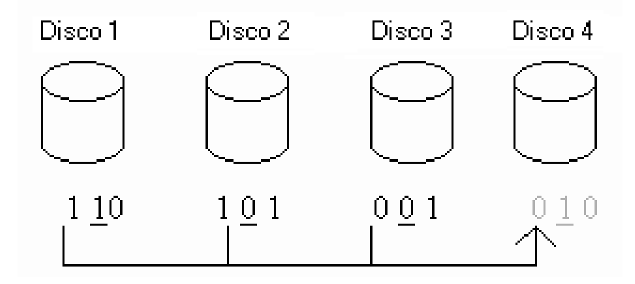
Para una solución que implique n discos, la información que debe escribirse se divide para ser distribuida entre los n-1 discos.

Por ejemplo, para escribir '110 101 001', se reparte en el bloque de intervalos constituido por cuatro discos.

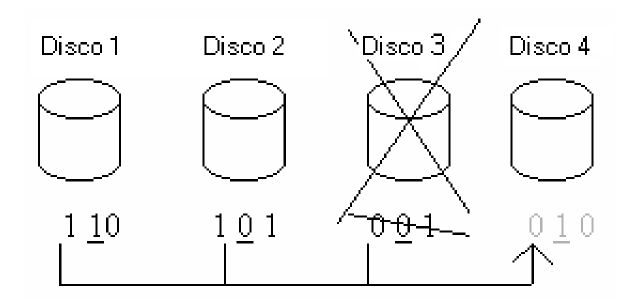
Para cada símbolo en enésima posición de cada disco, se calcula la información de paridad: lo que equivale a calcular el número de '1' para una posición dada y asignarle el enésimo intervalo, donde se almacenará la paridad, para que la determinación del número global de '1' sea par (paridad uniforme).

Así, si tomamos el primer símbolo de cada uno de los tres discos, obtendremos: '1 1 0'. Se determina el primer símbolo del disco 4 eligiendo '0', de modo que el número '1' sea par. De esta manera hay dos símbolos '1' entre los cuatro discos.

De la misma manera, para los símbolos que se encuentran en segunda posición, es decir, '1 0 0', se elige '1' como segundo símbolo en el último disco. Se obtiene así '0 1 0' como información de paridad para el disco 4. En caso de fallo de uno de los discos, por ejemplo el segundo, se recalcula la información perdida de la misma manera que si se tratara de información de paridad.



A partir de los discos 1, 2 y 4, se seleccionan los primeros símbolos de cada uno: '1 1 0'. Se calcula el símbolo necesario para obtener un número par de '1', es decir '0'.



Se efectúa la misma operación para los segundos símbolos y luego para los terceros. Se localizan '0 0 1', lo que nos permite reconstruir la información global representada como '110 101 001', y todo esto a pesar de que uno de los discos duros esté defectuoso.

El cálculo de paridad en el nivel más bajo es efectuado por una UO (Unidad Organizativa) exclusiva (XOR). De esta manera, la paridad del disco 4 es d4 = 110 XOR 101 XOR 001, o sea, 010. De este modo es más fácil obtener cualquier información, por ejemplo d3, a partir de los tres discos restantes. Por ejemplo, d3 = 110 XOR 101 XOR 010.

La UO exclusiva se basa en la lógica siguiente: 0 XOR 0 = 0, 0 XOR 1 = 1, 1 XOR 0 = 1, 1 XOR 1 = 0. Podemos entender la UO exclusiva como una suma binaria con posible pérdida de retención. En el lenguaje oral, podemos asociarlo con «Queso o postre» en un menú de restaurante, donde solo uno de los dos es una elección válida.

e. La neutralización de los sectores defectuosos

Este método permite garantizar el almacenamiento correcto de los datos en caso de sectores defectuosos. De hecho, todos los datos se escriben en segundo plano y luego son verificados. Cuando no se consigue escribir después de algunos intentos (es decir, cuando los datos que deben escribirse en la RAM no son los mismos que los escritos en el disco), el sector se marca como defectuoso y los datos se redirigen hacia un espacio reservado del disco. Y se deja de utilizar el sector marcado.

4. Soluciones de redundancia en servidor

Las soluciones de redundancia en servidor permiten dos funcionalidades que es necesario distinguir:

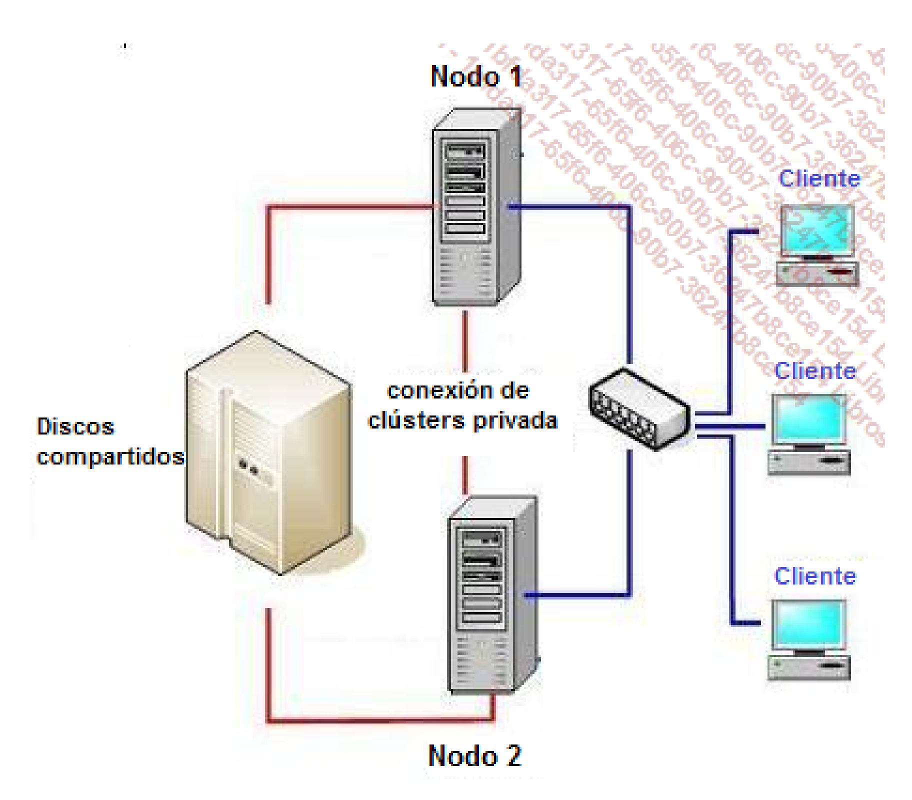
- La tolerancia a fallos.
- La distribución de carga.

Estas dos funciones pueden ejecutarse simultáneamente.

Este tipo de soluciones posibilita lo que se conoce como alta disponibilidad, ya que ofrece un servicio continuo a los usuarios, incluso en caso de problemas de sobrecarga.

a. La tolerancia a fallos

En este caso, varios procesos de un sistema operativo de servidores adaptado se ejecutan en distintos servidores. Esta tecnología se conoce como clúster de n nodos y define una solución que ejecuta n procesos de un mismo sistema operativo. Como ejemplo, en el siguiente recuadro esquematizamos la ejecución de un clúster de dos nodos.



Esquema de un clúster de dos nodos

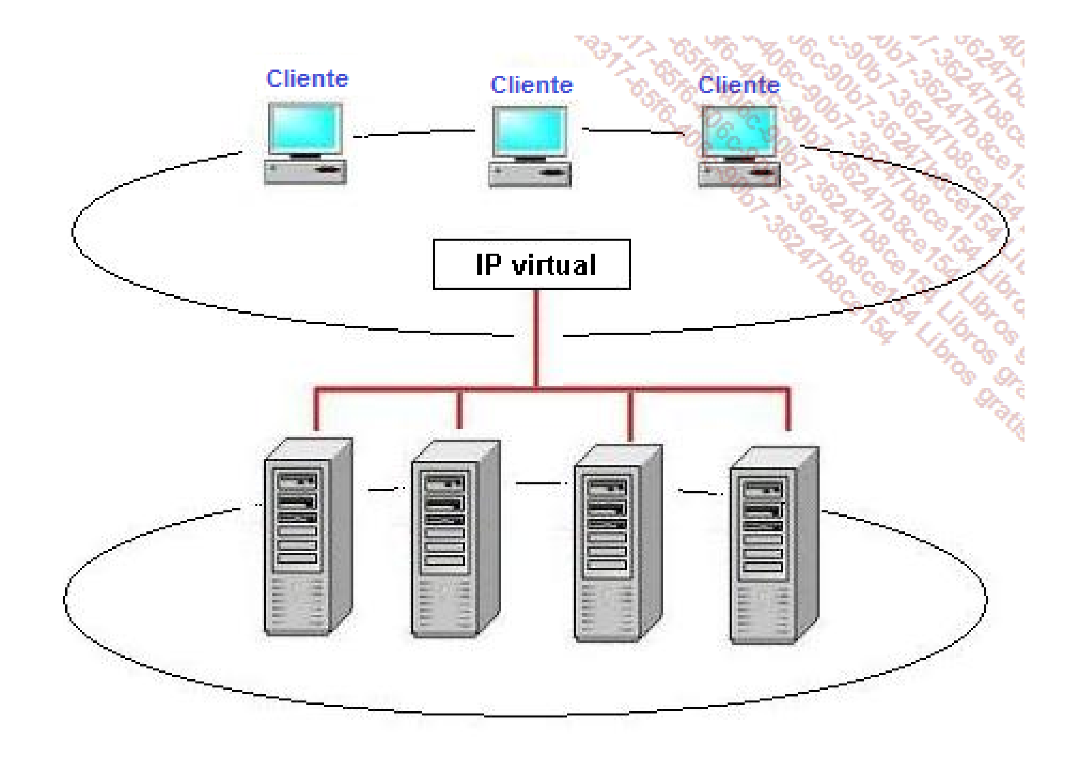
Esta tolerancia a fallos permite mantener el servicio para los usuarios. Por otra parte, es necesario que los datos se mantengan disponibles y actualizados, sea cual sea el servidor que falle.

Si estos datos se mantienen en los discos duros locales de los servidores, se puede poner en marcha una sincronización continua (replicación). Si no, es posible desviar los datos a un pool de almacenamiento compartido (infraestructura NAS).

En este sistema de redundancia de servidores, no todos responden obligatoriamente a las demandas de los usuarios. Este funcionamiento se reserva a las soluciones más evolucionadas. A menudo, un solo servidor ofrece de forma permanente sus servicios a los usuarios (servidor activo) y un segundo permanece preparado para tomar el relevo en caso de fallo del primero (servidor pasivo).

b. La distribución de la carga de red

El *Network Load Balancing* (NLB) no corresponde en realidad a una solución de hardware, en el sentido que se pueden utilizar ordenadores no dedicados al rol de servidores. Esta labor también es posible realizarla con PC que estén puestos en red.



Clúster de carga de red equilibrada

A pesar de que esta solución no es forzosamente la más fiable (con respecto a la utilización de verdaderos servidores), permite disminuir considerablemente los costes de adquisición y además puede constituir una solución interesante para el sector pyme.

El equilibrio de carga de red permite proporcionar una solución de alta disponibilidad avanzada. Es perfecta, por ejemplo, para servir sitios Web.

Una funcionalidad como esta permite adaptar los resultados vinculados a la aplicación, distribuyendo las peticiones de clientes entre los servidores que forman el clúster. Así pues, cuando el tráfico aumenta, es posible añadir servidores suplementarios al clúster.

Se puede implementar una funcionalidad de «Teaming» en un servidor cuando este posee varias interfaces de red. Ofrece una tolerancia a fallos e incluso una distribución de carga y simula, igual que el NLB, una interfaz virtual con un punto de entrada único. En este caso se

trata de duplicar las tarjetas de red, y no los servidores.

La virtualización como solución en sí misma

La virtualización es, sobre todo, una solución de consolidación, pero, además, un argumento que nos puede llevar a su implementación es la posibilidad de ofrecer fácilmente altos niveles de disponibilidad.

Una infraestructura virtual puede actuar a varios niveles para mejorar la disponibilidad de la solución:

- reduciendo considerablemente las interrupciones de servicios programados;
- evitando las interrupciones de servicios no programados;
- permitiendo un restablecimiento rápido después de una parada.

De hecho, las soluciones de virtualización en la actualidad permiten mover dinámicamente máquinas virtuales hacia diferentes servidores físicos, y esto, sin interrumpir el servicio. Así, para operaciones de mantenimiento del hardware, no es necesario implementar «ventanas de mantenimiento» correspondientes a periodos de interrupción de servicio, a menudo difíciles de planificar.

La virtualización propone igualmente numerosas ventajas ofreciendo un «teaming» de las interfaces de red o incluso de las rutas de acceso múltiples a los recursos SAN.

También es posible ofrecer una solución que cambie automáticamente cuando haya una incidencia, sin tener ninguna dependencia del hardware específico dedicado, ya que el usuario trabaja en las máquinas virtuales, independientes del hardware.

Las soluciones de software de servicios de clúster permiten igualmente una verdadera configuración de alta disponibilidad.

5. Política de respaldo

Para cada archivo creado o modificado, el sistema operativo asigna un bit de archivo o actualiza la fecha de la última modificación. A partir de ahí, es posible determinar qué archivos deben respaldarse.

Los productos Microsoft y Novell se basan en un atributo de archivo. Los sistemas Unix y Linux trabajan con las fechas de los archivos.

Una empresa determinará su política de respaldo para poder responder a varias cuestiones:

- ¿Cuáles son los archivos que deben respaldarse?
- ¿Con qué tipo de respaldo?
- ¿Cuándo efectuar las copias de seguridad?
- ¿En cuántos soportes?
- ¿Es más importante respaldar rápidamente o restaurar rápidamente?
- ¿Cuántas cintas se deben utilizar, de qué manera (rotación de las cintas)?

a. El respaldo completo

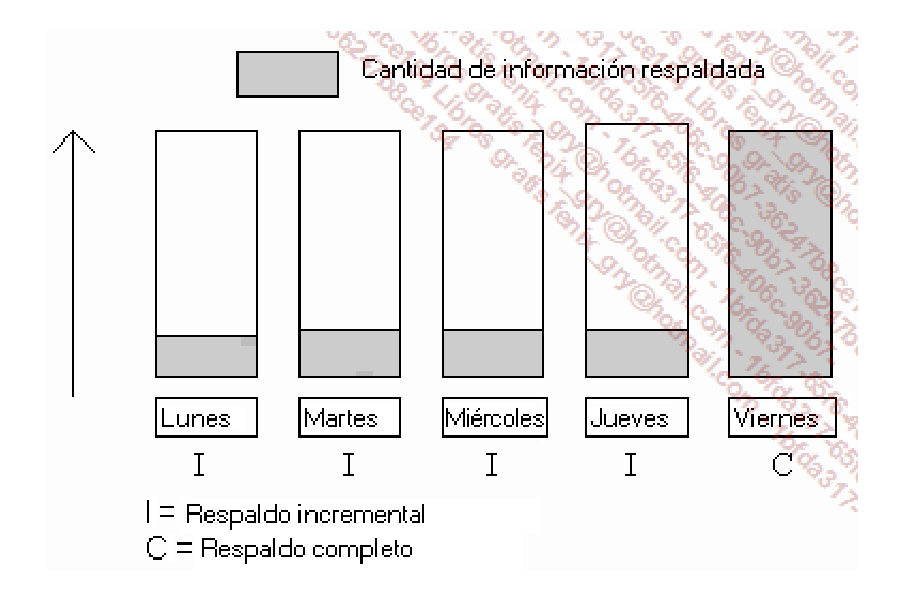
En un respaldo completo, los atributos de archivo se reinicializan para almacenar el hecho de que se ha grabado. Si se utiliza la fecha, se debe utilizar la del último respaldo que se guarda, de tal

modo que se puedan diferenciar los archivos que se respaldaron de los que aún no (fecha de la última modificación).

b. El respaldo incremental

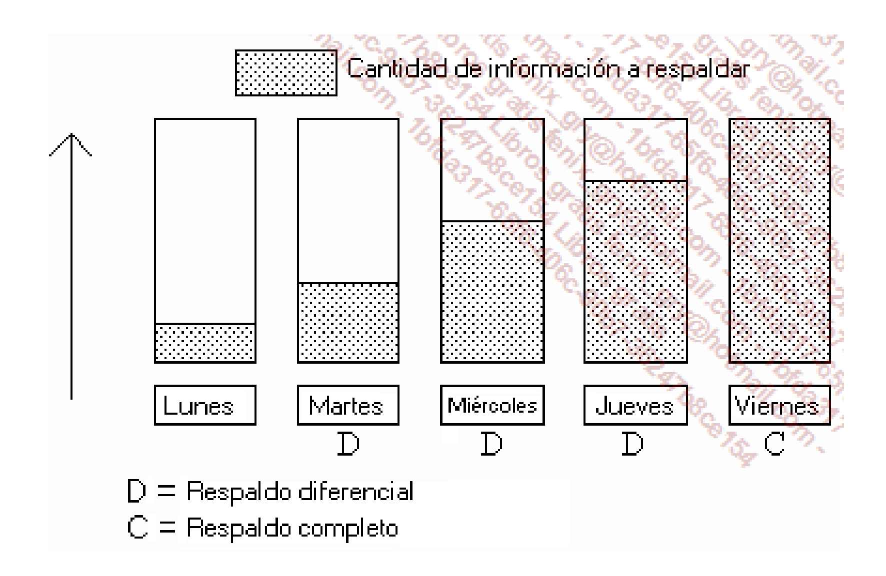
Esto tipo de respaldo marca los archivos como ya grabados. Se realiza, en general, diariamente, y tiene en cuenta las modificaciones del día anterior. Una política semanal consiste, por ejemplo, en efectuar un respaldo completo los viernes y una copia incremental el resto de los días.

Esta política minimiza la duración de la copia diaria. En contraposición, en una restauración completa hasta el último jueves, por ejemplo, sería necesario restaurar la cinta del viernes anterior, más las cuatro cintas correspondientes a cada uno de los días de esa semana.



c. El respaldo diferencial

Este tipo de respaldo (a menudo diario) no necesita reinicializar los atributos de los archivos para indicar que ya se registraron. Por lo tanto, para cada nuevo respaldo diferencial, se tienen en cuenta las modificaciones anteriores y las del mismo día.



Esta política minimiza el tiempo de restauración, puesto que solo requiere dos cintas (la completa más la última diferencial). Aunque tiene el inconveniente de que la copia diaria es cada vez más larga.

Podemos citar como principales soluciones de copias de seguridad: ARCserve (CA), Backup Exec o Netbackup (Symantec), Networker (EMC), Time Navigator alias TiNa (Atempo), Tivoli

Storage Manager alias TSM (IBM).

6. Continuidad y reanudación de la actividad en caso de siniestro

a. Principios

El sistema de información de una empresa no está exento de incidentes, que pueden afectar a uno o más equipos, o incluso de un accidente o problema grave, por ejemplo en la sala de servidores. El coste implicado puede tener consecuencias desastrosas. Se pueden poner en práctica planes y métodos de seguridad para garantizar la continuidad o la reanudación de la actividad en tales casos.

La reacción después de un daño debe ser proporcional a este. Se deberá prever con anterioridad una serie de medios que sucesiva y escaladamente vayan actuando. El primer punto consiste en la redacción de un balance de impacto en la actividad (BIA), que contenga:

- el análisis de los costes financieros;
- la identificación de las aplicaciones críticas;
- la determinación del tiempo necesario para la reanudación de la actividad;
- el detalle de la infraestructura del sistema de información;
- la lista de los usuarios críticos.

El BIA está destinado a facilitar las distintas decisiones que se deban tomar, siempre difíciles después de un accidente. Pueden completarse con:

- soluciones de emergencia y su activación;
- el nombramiento de un departamento de crisis, con especialistas de cada sector, cuyo peritaje se solicitará en ese momento;
- la puesta en marcha de un plan de continuidad de la actividad (PCA) o de un plan de reanudación de la actividad (PRA);
- protocolos y pruebas necesarios.

b. El plan de continuidad de la actividad (PCA)

El PCA (o BCP - *Business Continuity Planning*) define el conjunto de acciones que garantizan la continuidad de la empresa después de un incidente grave. Debe acompañarse de medidas urgentes; es un plan a corto plazo.

Permite cuantificar las necesidades para poder continuar la actividad, incluso en un estado degradado del sistema, después de una interrupción corta, de algunos segundos a decenas de minutos. Se compone de:

- medidas preventivas;
- redistribución de las principales tareas;
- contractualización con los proveedores y aseguradoras;
- degradación previsible del sistema;
- procedimientos y pruebas.

c. El plan de reanudación de actividad (PRA)

El plan de reanudación de actividad (o BRP - *Business Recovery Plan*) es el conjunto de los procedimientos que permiten la reanudación de la actividad en un sitio de emergencia después del incidente. La interrupción se calcula desde algunas horas hasta algunos días, hasta que sea posible la aplicación del PCA.

Cada actor del sistema y cada actividad de la empresa es objeto de reanudaciones específicas. Debe haber un PRA por sistema, por entorno, por aplicación, por ámbito de actividad o por sitio, según la política de seguridad definida.

El PRA está constituido por distintos procedimientos.

Plan de preparación

El plan de preparación determina el entorno necesario para la reanudación. Describe la estructura física del lugar provisional (medios informáticos, red, telecomunicaciones, logística...). Describe también el mapeado lógico de las aplicaciones y los medios humanos que deben solicitarse.

Plan de ejecución

La definición y la planificación de las etapas de reanudación están en este plan de ejecución, que incluye una descripción de las actividades y responsabilidades de los participantes, así como las acciones que deben emprenderse.

Plan de recuperación

Este procedimiento prevé la reinstalación de las aplicaciones y la restauración de los datos. Debe incluir una estimación del tiempo necesario para restablecer el funcionamiento.

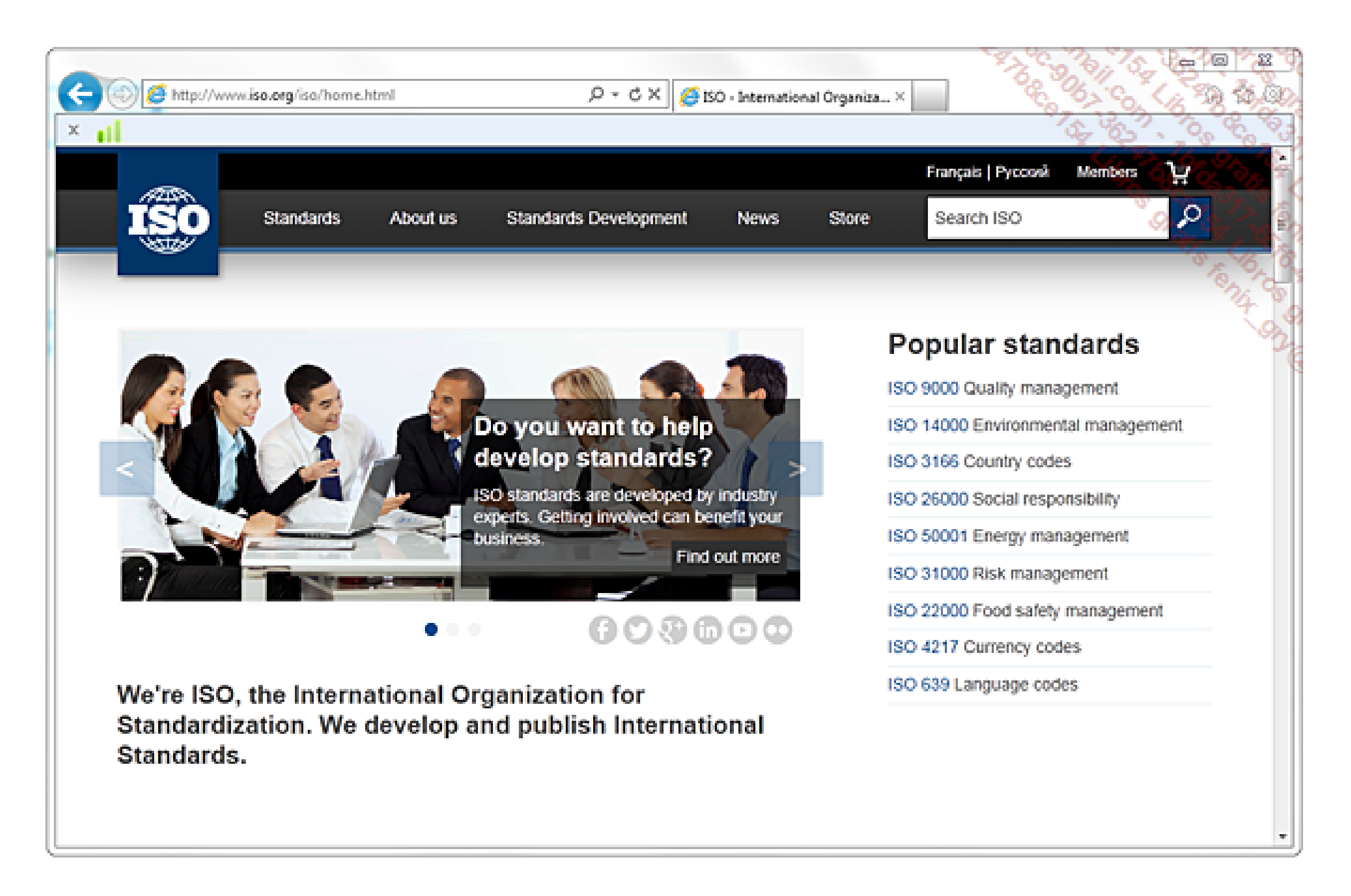
Validación y actualización

Las pruebas de validación de procedimientos tampoco deben olvidarse. Así pues, se puede realizar una prueba completa al finalizar la ejecución del PRA.

Y, por supuesto, a todo cambio importante dentro del sistema de información debe corresponder una actualización de estos procedimientos.

Modelo OSI

Un aspecto importante en la apertura de las redes fue la instauración de un modelo de referencia, el modelo OSI del ISO. Este define un modelo de red en siete capas, presentes en cada equipo que desee conectarse. Cada capa dispone de funcionalidades que le son propias y presta servicio a las capas inmediatamente adyacentes. Aunque el modelo OSI se utiliza muy poco, sirve de referencia para definir el nivel de funcionamiento de un componente de red. Así, hoy en día, y de manera paradójica, el TCP/IP se utiliza de forma generalizada, e incluso cuando se habla de este protocolo se le asocia con las capas del modelo OSI (10 años más reciente que el modelo TCP/IP).

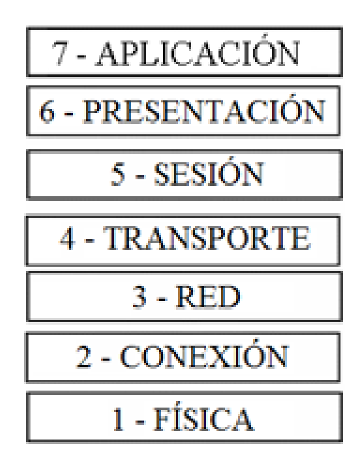


Sitio web de ISO: www.iso.org

1. Principios

El organismo ISO definió en 1984 un modelo de referencia, llamado *Open System Interconnection*(OSI), destinado a estandarizar los intercambios de información entre dos máquinas. Con él, se definió lo que debía ser una comunicación de red completa. El conjunto de procesos se divide así en siete capas jerárquicas.

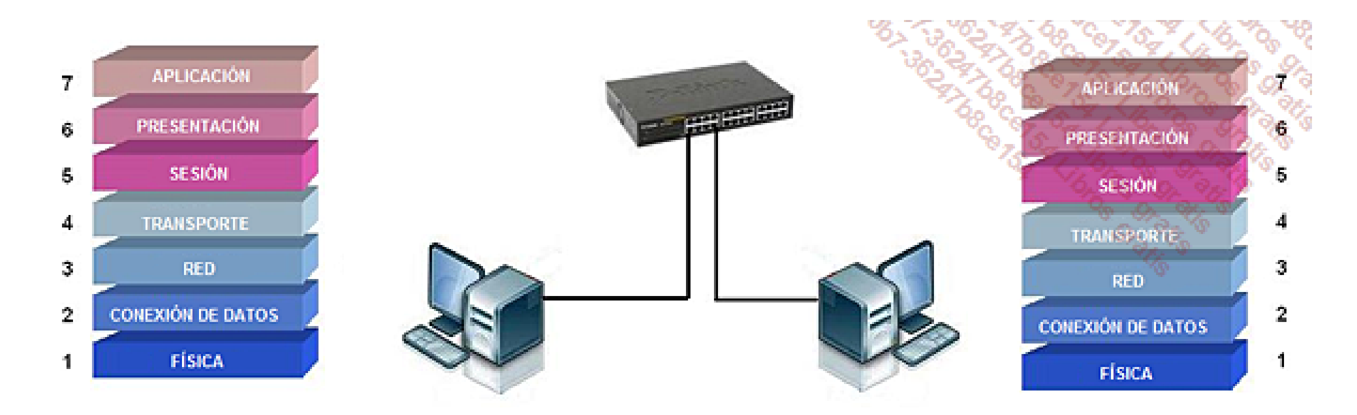
Este modelo define de forma precisa las funciones asociadas a cada capa. Cada una de ellas se comporta como un prestador de servicios para la capa inmediatamente superior. Para que una capa pueda hacer una petición o enviar datos al nivel equivalente, debe «constituir» la información y hacerla pasar a través de todas las capas inferiores, cada una de las cuales le añadirá un encabezamiento específico, convirtiéndose en una especie de tren. Una vez transferida, se descodifica la información y se liberan la petición o los datos que originaron el proceso.



Las siete capas del modelo OSI

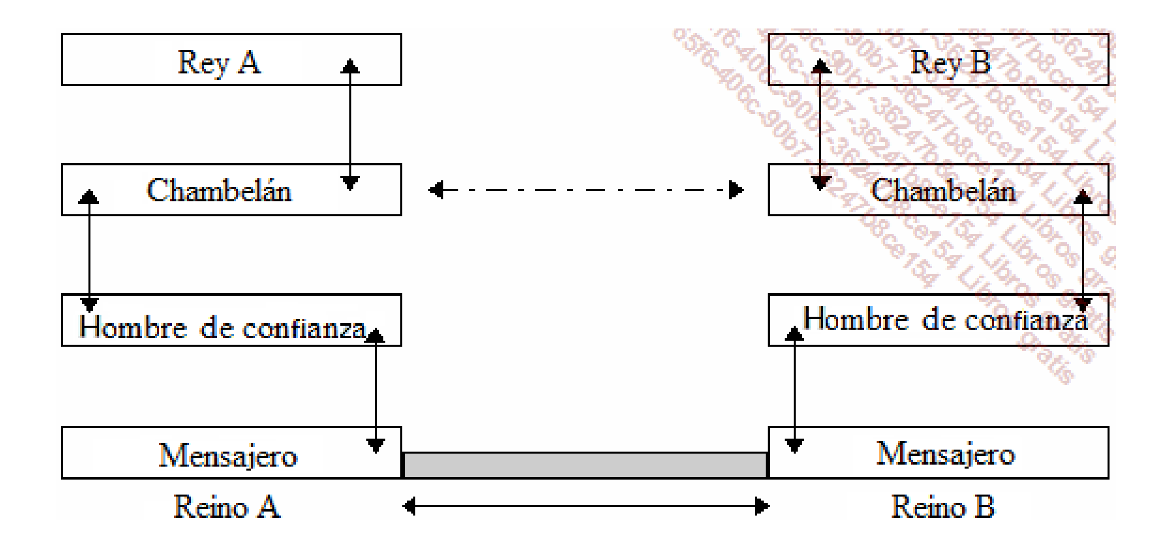
2. Comunicación entre capas

Cada capa garantiza una función muy precisa durante la transmisión de los datos. Se trata, de hecho, *de divide y vencerás*. La capa N utiliza la capa N-1 y proporciona servicios a la capa N+1.



El modelo OSI y las siete capas

Podríamos comparar este mecanismo con el de dos reyes de la Edad Media que desearan intercambiar una misiva entre sus dos reinos, A y B. El primer rey entrega un pergamino a su gran chambelán, encargado a su vez dar las consignas a su hombre de confianza, quien a su vez entrega las consignas a un mensajero para transportar el precioso pergamino hacia la comarca del rey destinatario.



Vista esquemática del modelo

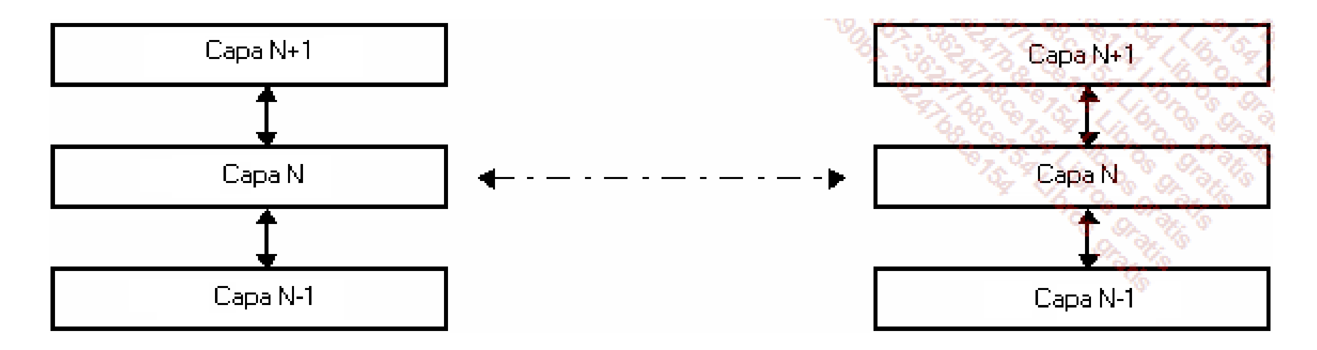
El mensajero del reino B recibe el pergamino con consignas procedentes del mensajero del reino A. Estas consignas le piden hacer llegar el pergamino al gran chambelán del rey B. El gran chambelán B lee finalmente las consignas procedentes del gran chambelán A, que le pide entregar el pergamino al rey B. El rey B puede así leer la misiva del rey A.

Todo pasa como si una capa de red de un ordenador dialogara directamente con la capa homóloga del otro ordenador (como lo hacen los grandes chambelanes en nuestro ejemplo).

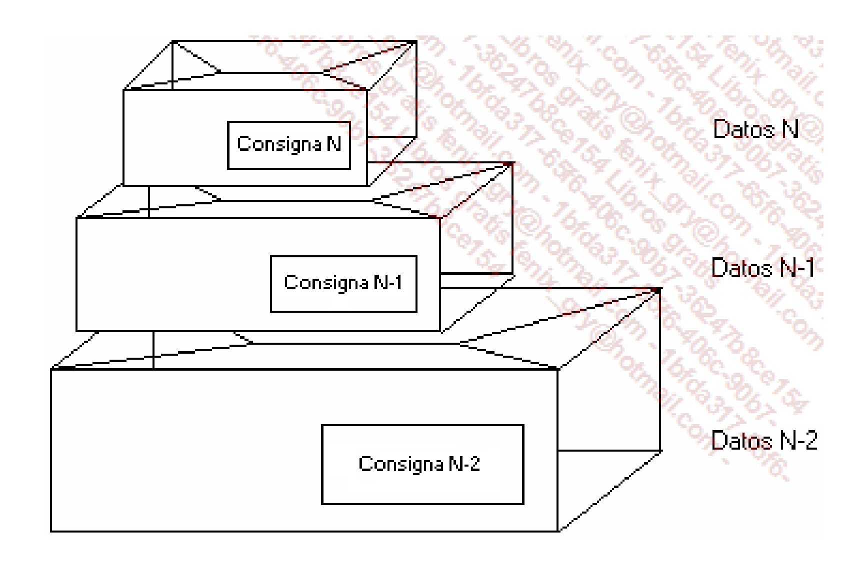
En realidad, el transporte de la misiva es posible porque la información vuelve a bajar hasta el mensajero, que puede entonces transportar los datos hacia el otro reino (aquí el mensajero es el soporte físico que sirve para transportar la señal que cifra los datos que se deben emitir). Una vez la información llega a su destino, sube por las capas y se interpretan las consignas sucesivas de las capas homólogas.

3. Encapsulación y modelo OSI

Cuando un capa de red quiere dialogar con su capa homóloga, no tiene otra opción que hacer que vuelva a bajar la información añadiendo consignas para la capa del destinatario. Así, el encabezamiento y los datos de una capa N se convierten en los datos de la capa N-1. Esta capa N-1 construye un encabezamiento (las consignas). Este encabezamiento y estos datos se convierten en los datos de la capa N-2.



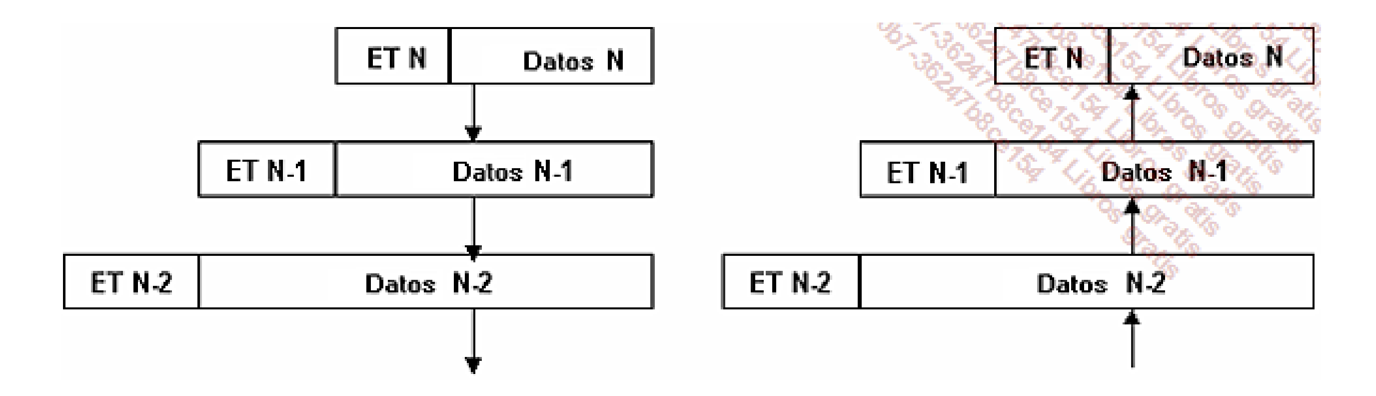
A este proceso lo llamamos encapsulación. Es como si se colocaran datos dentro de una caja de consignas para ella misma. Esta caja y estas consignas se colocan a continuación en una caja más grande con nuevas consignas, y así sucesivamente.



Encapsulación y modelo OSI

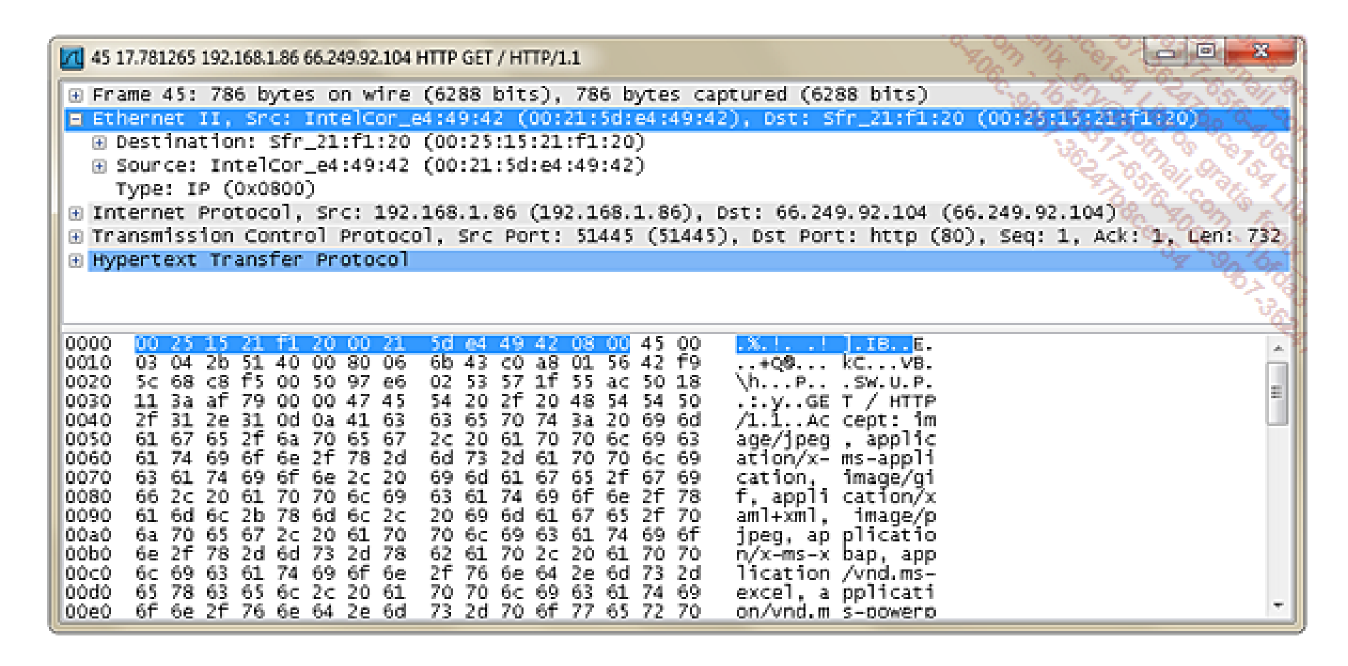
Cuando el paquete llega al destinatario, se leen las consignas y se abre la caja. La caja que está dentro de la más grande se transmite según las consignas que han llegado.

En el siguiente esquema, se han asociado las consignas a los encabezamientos de los diferentes niveles (ET N, ET N-1, ET N-2).



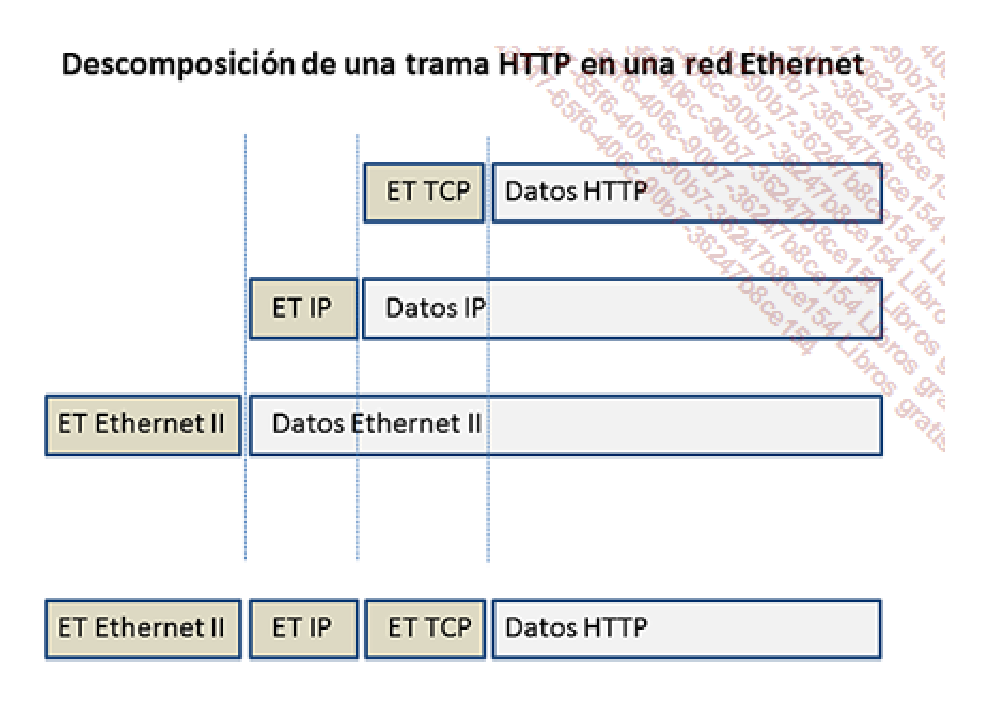
Encapsulación de una capa N en la capa N-1

Por ejemplo, vea lo que se obtiene examinando una trama HTTP si se utiliza una herramienta como Wireshark de captura de tramas de red:



Ejemplo de trama HTTP capturada

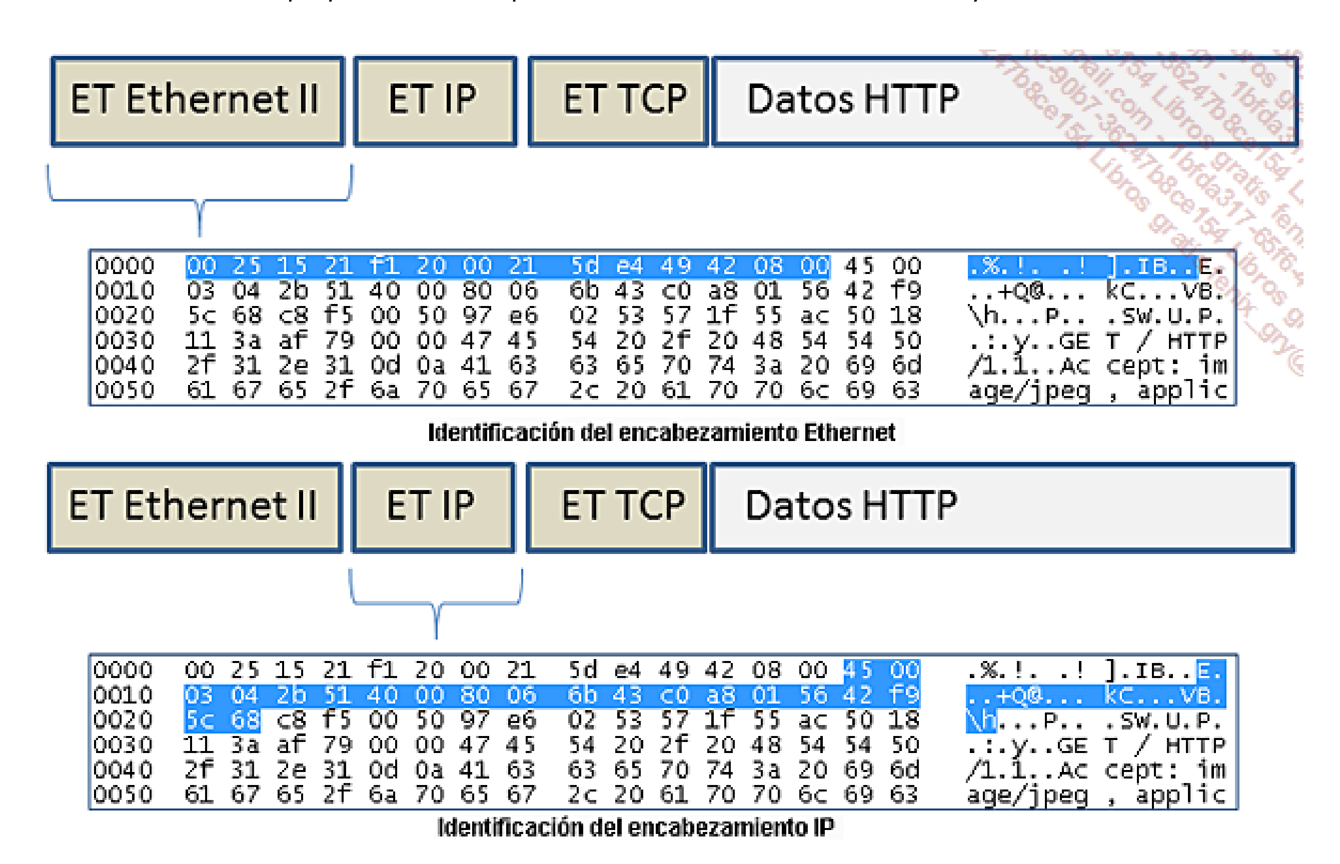
La trama HTTP está encapsulada como datos TCP, en la capa TCP. El encabezamiento TCP añadido a los datos TCP forman los datos IP. Finalmente, el encabezamiento IP y los datos IP forman los datos Ethernet:



Relación entre las capas, los encabezamientos y los datos

La trama se ve finalmente como una secuencia de encabezados, seguidos de los datos de la capa «más alta».

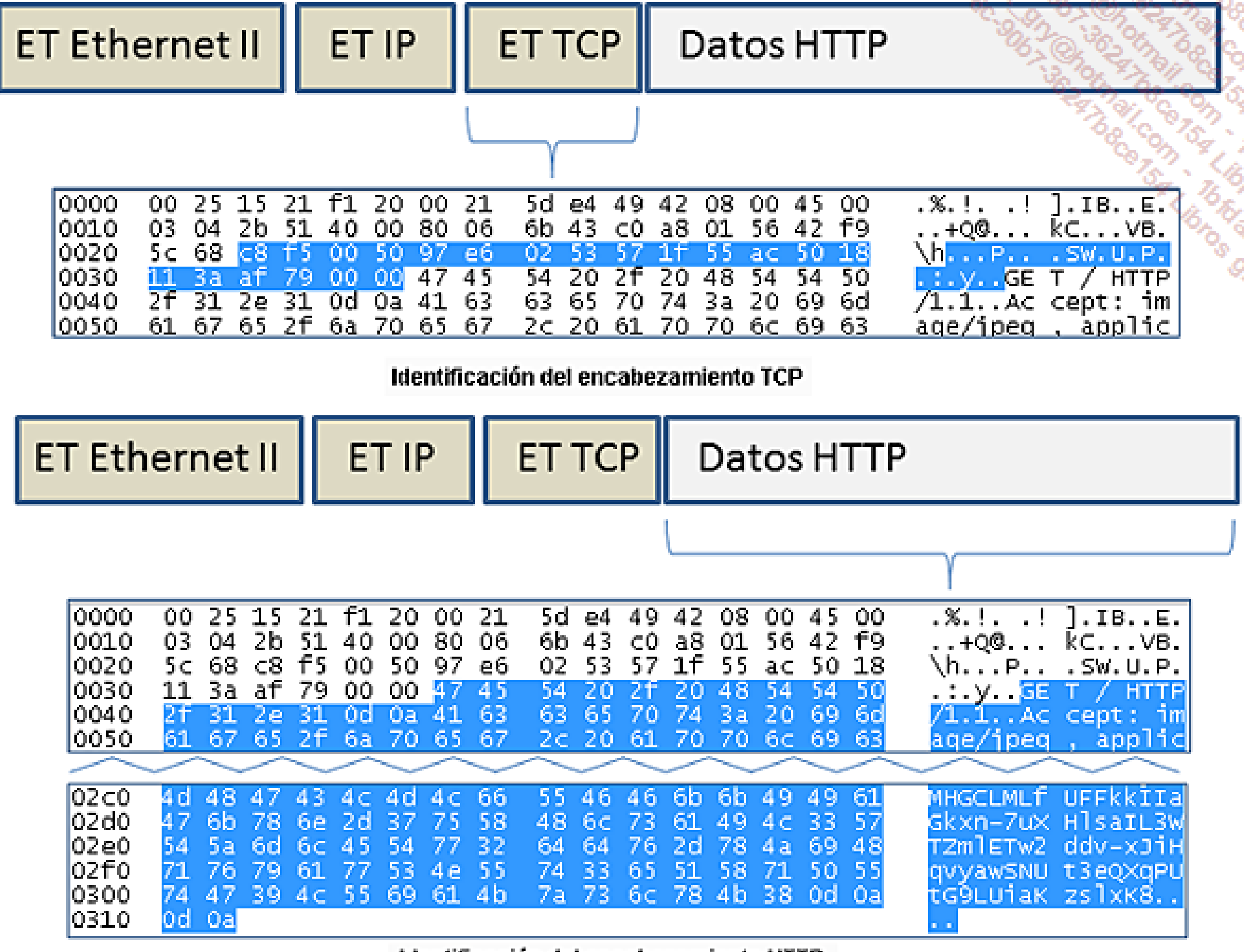
Observando la información ofrecida por el analizador de tramas, es posible identificar las diferentes partes de la trama. Aquí puede verlas para el encabezamiento Ethernet y el encabezamiento IP:



Identificación del encabezamiento Ethernet

Identificación del encabezamiento IP

Lo mismo ocurre para la parte del encabezamiento TCP y los datos HTTP:



Identificación del encabezamiento TCP

Identificación del encabezamiento HTTP

4. Protocolos

El modelo OSI divide y especifica las funciones propias de la comunicación a través de siete capas lógicas.

La materialización de las capas del modelo teórico toma la forma de protocolos. En cada protocolo se aplican diferentes funciones definidas por el modelo.

Un protocolo constituye, por tanto, un conjunto de reglas de comunicación. Estas reglas establecen el formato de transmisión de los datos a través de la red.

El ideal teórico del modelo OSI consiste en implantar un protocolo por capa.

En realidad, algunos protocolos operan en varias capas, otros en una capa y algunos solo en una parte de algunas capas, tal como las define el modelo OSI.

De hecho, no se debe olvidar que este modelo se creó cuando ya existían muchos otros protocolos, por lo que algunos fabricantes se adaptaron al modelo, mientras que otros siguieron utilizando sus protocolos sin modificarlos.

5. Papel de las distintas capas

Cada capa de red definida por el modelo tiene un papel concreto que va desde el transporte de la señal que cifra los datos a la presentación de la información para la utilización por parte del destinatario.

a. La capa Física

Su papel es la transmisión bit a bit a través del soporte, entre el emisor y el receptor, de las señales eléctricas, electromagnéticas o luminosas que codifican los datos digitales (0 o 1).

Puesto que define el modo de propagación de la señal, esta capa administra, si es preciso, los circuitos físicos. Los componentes de hardware, como los módems (modulador/demodulador), los repetidores o los conectores de tarjetas de red, como por el ejemplo el RJ45, se colocan en este nivel.

b. La capa Conexión (o Conexión de datos)

En esta capa los datos digitales se transforman en señal. Los bits de datos se organizan en tramas. Se crea un encabezamiento en el que se puede identificar al emisor y al destinatario por su dirección física.

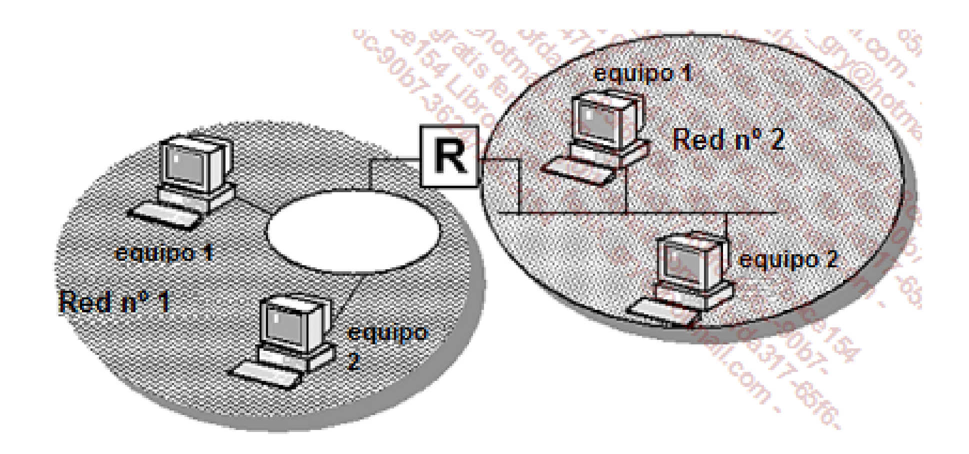
En esta capa se añade un código de redundancia cíclica (CRC - *Cyclic Redundancy Check*) que permite detectar algunos problemas de transmisión. Así, el destinatario de una trama recalcula el CRC y lo compara con el que se transmitió. Si hay alguna diferencia, se rechaza la trama.

El modelo OSI ofrece la implementación de High level *Data Link Control* (DLC) para este nivel de capa.

También podemos citar el protocolo *Synchronous Data Link Control* (SDLC), desarrollado por IBM para su secuencia de protocolos *System Network Architecture* (SNA), o también *Low Access Procedure Balanced* (LAP-B), desarrollado por el CCITT (Comité Consultivo Internacional Telegráfico y Telefónico) para su modelo. Este último es el que finalmente se utiliza para los protocolos X.25.

c. La capa de Red

Es esta capa se escoge la mejor ruta (cuando existen varias) para llegar al destinatario. Mientras que la dirección física sirve para identificar un periférico local, una dirección lógica permite hacer referencia a un componente de manera global. Por eso, algunos protocolos identifican los periféricos de la red asignándoles un número de red, así como un número de puesto en esa red.



La capa de red

Para llegar a un destinatario, se calcula un coste que puede depender de varios parámetros (número de redes que deben cruzarse, duración del transporte, coste de la comunicación, saturación de la línea, etc.). Mediante la comparación de los distintos costes se determina qué ruta es la mejor.

En función de los protocolos, el bloque puede llamarse mensaje, datagrama, célula o incluso paquete, como en *Internet Protocol* (IP).

d. La capa de Transporte

Es el núcleo del modelo OSI. En esta capa, se ponen en marcha distintos mecanismos para

establecer el modo conectado, es decir, un medio para garantizar que la información se transmite sin problemas. El primer nivel de conexión consiste en un acuse de recibo sistemático de todos los paquetes recibidos, y esto, en un plazo determinado (dos veces la duración de ida y vuelta normalmente necesaria), porque, de lo contrario, el paquete se da por extraviado y se vuelve a transmitir. Además, el modo conectado ofrece una conexión para la capa superior, como si se tratase de un enlace punto a punto.

Así como la capa de red elige la mejor ruta a través de una visión global de la intrarred, la capa de transporte añade un mecanismo de control relativo a la fiabilidad de los datos recibidos.

El protocolo más conocido a este nivel es *Transport Control Protocol* (TCP).

e. La capa de Sesión

Esta capa también administra un modo conectado. En este nivel se gestionan los puntos de sincronización, permitiendo así, a través de la protección de contextos y subcontextos, la reanudación en caso de error.

Es la capa que suele administrar la conexión a un recurso compartido en la red.

Los comandos MAP o NET USE, para los sistemas Novell Netware y Microsoft Windows, permiten crear una conexión con un recurso de tipo carpeta o directorio, asociándole una letra de unidad lógica.

Las llamadas a procedimientos remotos, *Remote Procedure Call* (RPC), constituyen un protocolo de este nivel.

f. La capa de Presentación

Esta capa garantiza la estandarización de los datos: parámetros internacionales, páginas de códigos, distintos formatos...

Es el papel que asume, por ejemplo, el lenguaje HTML (*HyperText Markup Language*).

Esta capa también puede hacer uso de funciones de codificación y de compresión. Codificaciones como MIME (*Multipurpose Internet Mail Extensions*), ASCII (*American Standard Code for Information Interchange*) o ASN.1 (*Abstract Syntax Notation number One*) se pueden utilizar en esta capa.

g. La capa de Aplicación

Esta capa garantiza la interfaz de comunicación con el usuario a través de los programas informáticos adecuados.

También administra la comunicación entre aplicaciones, al igual que el correo electrónico.

Se pueden citar algunas de las numerosas opciones disponibles, como *File Transfer Access and Management* (FTAM), *Common Management Information Protocol* (CMIP), que permite efectuar un seguimiento de los recursos o administrarlos a distancia. *Message Handling Systems* (MHS) o X.400 es un método estandarizado internacional para el transporte de mensajes. X.500 o Directory Services permiten administrar una base de datos distribuida de manera estándar.

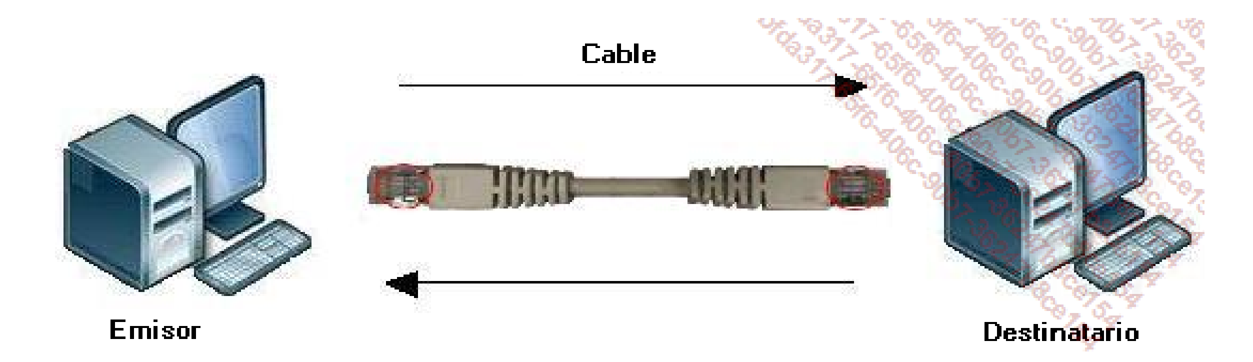
Enfoque pragmático del modelo de capas

Ahora vamos a examinar otro enfoque de un modelo de red en capas, concentrándonos aún más en el papel de cada una de las capas. Vamos a comenzar por examinar una comunicación de punto a punto entre dos periféricos, imaginándonos, por ejemplo, dos ordenadores conectados a través de un cable. Poco a poco, vamos a ir haciendo más complejo el entorno de interconexión añadiendo ordenadores, luego componentes de interconexión, para encontrarnos finalmente con una red compleja de ordenadores interconectados como Internet. El objetivo es comprender mejor este modelo de capas, porque la dificultad de comunicar dos entidades en un entorno heterogéneo es grande.

1. Nivel 1 - capa Física

Imaginemos, en primer lugar, dos ordenadores autónomos que desean compartir información por medio de un simple cable.

En esta representación, los dos ordenadores se conectan directamente uno al otro: es decir, una conexión punto a punto, igual que ocurre en una conexión telefónica, en la que, una vez establecida, los dos puestos podrán intercambiar datos simultáneamente, sin necesidad de precisar quién es el destinatario. ¡De hecho, no hay ambigüedad respecto a quién debe recibir los datos: es el que se encuentra al otro lado del cable!



Nivel 1: punto a punto físico

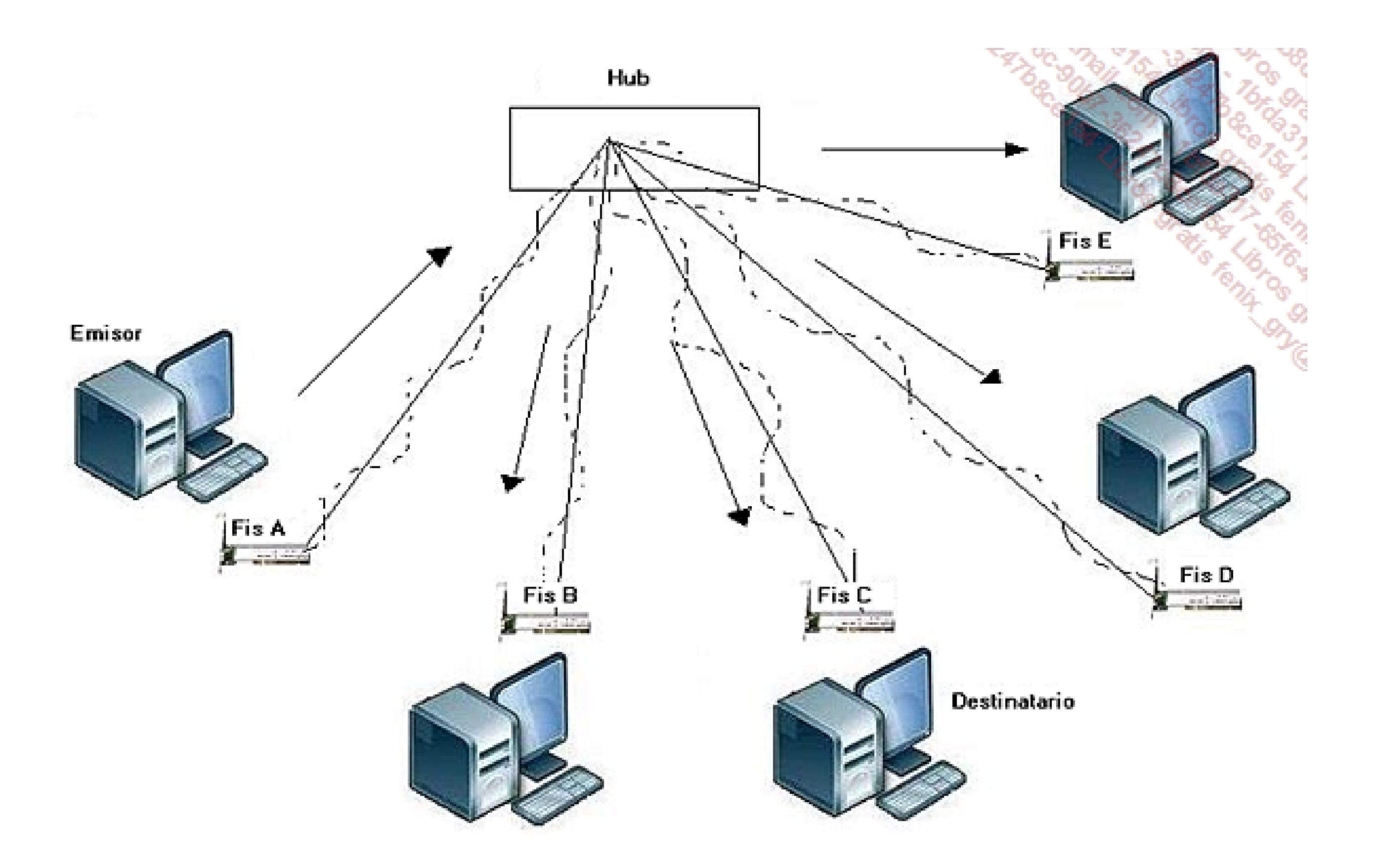
Por eso, en esta configuración, no es necesario ningún identificador y directamente se enruta la información hacia el destinatario que está al otro lado del canal de comunicación.

En este tipo de conexión punto a punto, es necesario utilizar un cable cruzado.

2. Nivel 2 - capa de Conexión de datos

En este nivel vamos a examinar el ejemplo de un entorno de red local: Ethernet en estrella con par trenzado.

En esta fase no es primordial comprender perfectamente la tecnología de red utilizada para ilustrar la explicación teórica, en este caso Ethernet. Este protocolo lo estudiaremos con más detalle más adelante.



Nivel 2: red Ethernet en estrella

Como se ve en la ilustración, todos los ordenadores están equipados con una tarjeta de red. Esta tarjeta sirve para comunicarse con el resto de los recursos conectados a esta red. Cada una de ellas es una especie de interfaz entre el interior del ordenador (el sistema operativo y la configuración de programas de la red) y el exterior de este.

La parte de software se denomina controlador. Permite, como veremos a continuación, establecer la relación con las capas de software superiores.

La relación con la capa Física se realiza mediante el conector presente en la tarjeta de red. Es esta última la que actúa como componente de interconexión.

Cuando un ordenador desee enviar datos, podrá hacerlo en el momento oportuno, aunque eventualmente deba esperar su turno, utilizando su tarjeta de red.

Con esta configuración, la señal que corresponde a los datos se emitirá a través de la tarjeta de red emisora al resto de tarjetas de red presentes. La señal se difundirá, así, como si se tratara de un grifo que se abre para abastecer a las otras tarjetas de red.

Contrariamente a lo que pasaba en el nivel anterior, donde la comunicación era directa (de punto a punto), para el nivel 2, debemos definir identificadores específicos.

Imaginemos que nos encontramos en un lugar atestado de gente; a pesar del barullo de la muchedumbre, logramos localizar a un amigo y lo llamamos. En ese momento, varias personas se dan la vuelta para saber quién llama a esa persona. A continuación, solo nuestro amigo sigue escuchando el mensaje que le transmitimos oralmente.

Por tanto, es necesario determinar, en cada trama enviada, a quién está dirigida la información. El emisor de la información se da a conocer y su identificador se registra en esta trama. Para ello es necesario un sistema de denominación de las partes. El enlace con la tarjeta de red se denomina direccionamiento físico.

Todas las tarjetas de red Ethernet disponen de una dirección física, llamada también dirección MAC (*Medium Access Control*), que viene a ser su propio identificador de nivel 2.

En el siguiente ejemplo, se ha efectuado una solicitud de información en la interfaz de comandos de Windows.

```
Adaptador Inalámbrico Conexión inalámbrica:
   Sufijo DNS específico para la conexión. . . :
   Descripción . . . . . . . . . . . . . . . . : Intel(R) WiFi Link
5100 AGN
   Dirección Física . . . . . . . . . . . . : 00-21-5D-E4-49-42
   DHCP habilitado. . . . . . . . . . . . . : No
   Configuración automática habilitada. . : Sí
   Vínculo: dirección IPv6 local . . . . .: fe80::a803:4bc3:61c9:909%13(Preferido)
   Dirección IPv4. . . . . . . . . . . . .: 192.168.1.86(Preferido)
   Máscara de subred. . . . . . . . . . . : 255.255.255.0
   Concesión obtenida . . . . . . . . . . : martes, 15 de marzo de 2011 16:08:09
   La conexión expira . . . . . . . . . . : miércoles, 16 de marzo de 2011 16:08:09
   Puerta de enlace predeterminada. . . . : 192.168.1.1
   Servidor DHCP. . . . . . . . . . . . . : 192.168.1.1
   IAID DHCPv6. . . . . . . . . . . . . . : 335552861
   DUID de cliente DHCPv6 . . . . . . . . : 00-01-00-01-13-B2-DB-
FE-00-21-70-DB-10-27
   Servidores DNS. .  . . . . . . . . . . : 192.168.1.1
   NetBIOS sobre TCP/IP . . . . . . . . . : Deshabilitado


Adaptador Ethernet Conexión de área local :
   Estado de los medios . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión : ULi PCI Fast Ethernet Controller
   Descripción. . . . . . . . . . . . . . : Intel(R) 82567LM
Gigabit Network Connection
   Dirección física . . . . . . . . . . . : 00-21-70-DB-10-27
   DHCP habilitado. . . . . . . . . . . . : No
   Configuración automática habilitada. . : Sí
```

Observe que en este ejemplo aparecen dos tarjetas de red, cada una con un identificador diferente.

El identificador aparece con el nombre *Dirección física*.

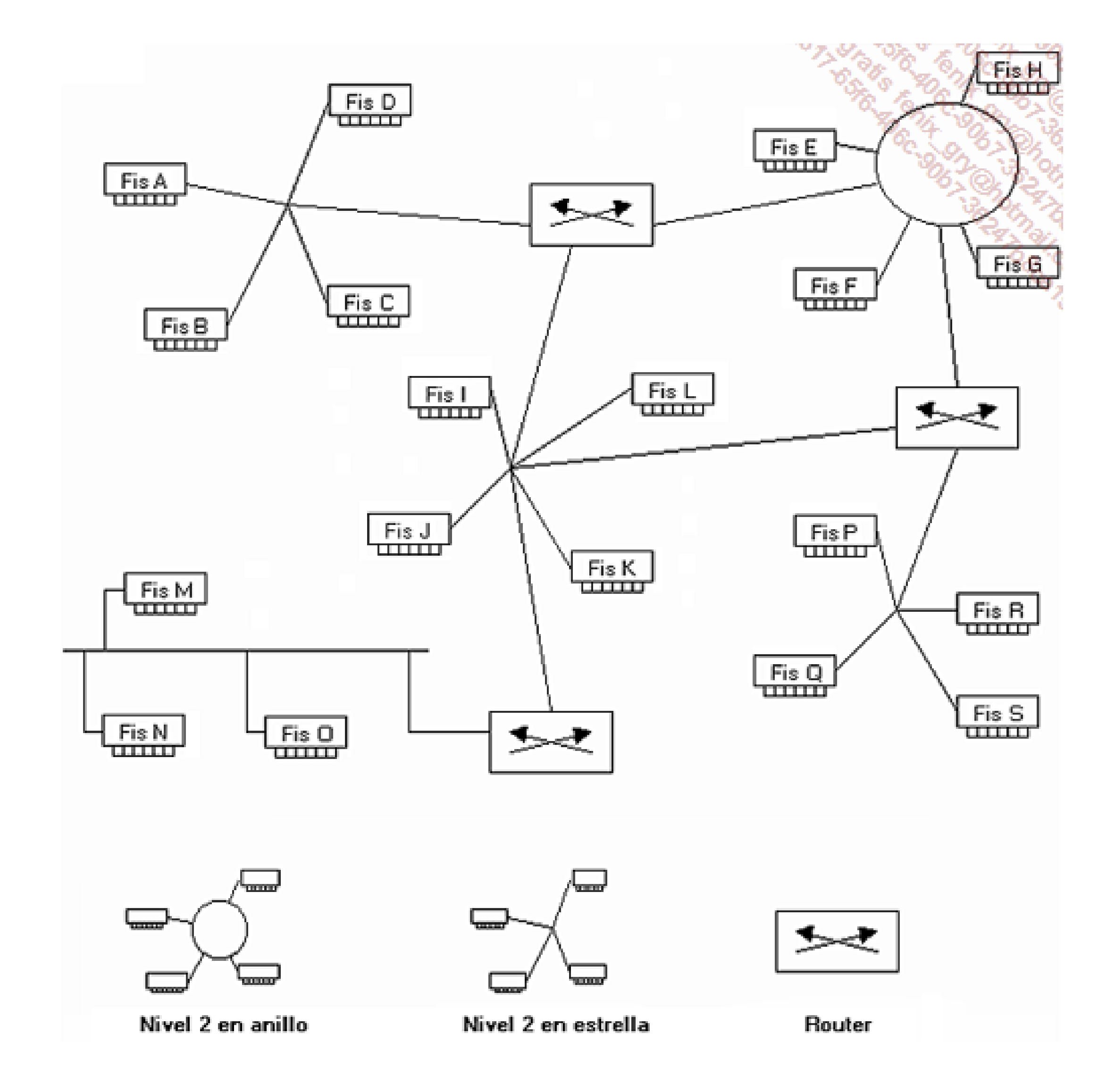
Los niveles 1 y 2 forman, a menudo, una sola y única capa para el administrador de red, llamada de base. Esto procede del hecho de que en el modelo de protocolos TCP/IP que a continuación se aplica (con diferencia el más frecuente), pero anterior al modelo OSI, forman una única capa llamada Interfaz de red.

El nivel 2 se refiere a un entorno donde el hardware (tarjetas de red, *hubs*) y la gestión del acceso al soporte físico siguen siendo los mismos. Una red de nivel 2 se calificará por su velocidad, con tramas cuya longitud máxima y mínima están establecidas.

3. Nivel 3 - capa de Red

a. Principios

Este nivel permite la interconexión de redes físicas diferentes. En el modelo TCP/IP, es en la segunda capa, llamada Internet, donde se encuentra el Internet Protocol (IP).



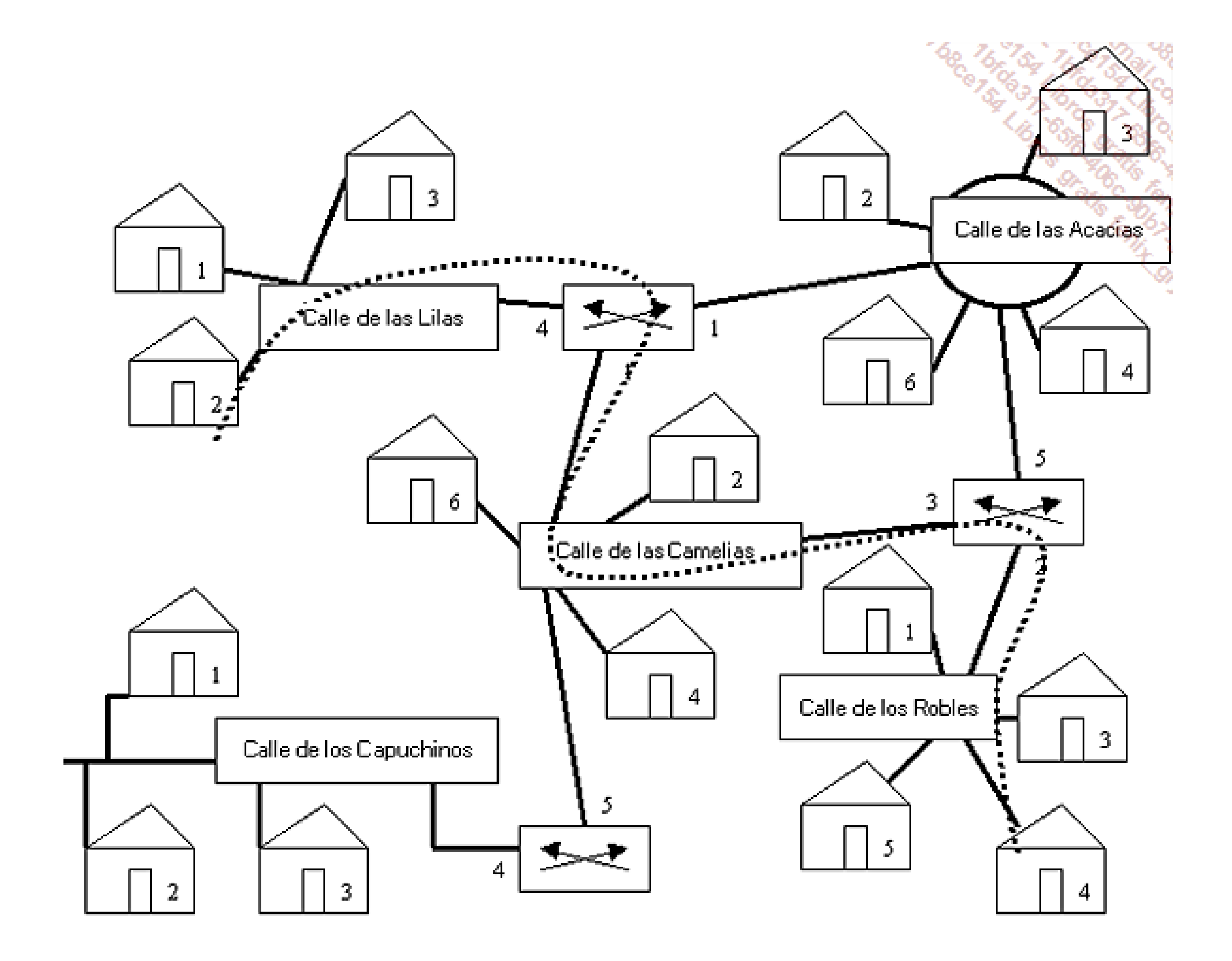
Nivel 3: interconexión de red de nivel 2

b. La dirección lógica

Este nivel es un poco más complejo. Se introduce una dirección lógica, complementaria a la dirección física de nivel 2. El concepto de dirección lógica define una descomposición jerárquica a un nivel: una dirección está compuesta por un número de red, así como por un número de equipo en la red.

Por ejemplo, en una dirección de tipo IPv4 192.168.1.100, el identificador de red lógico es 192.168.1 y el de equipo, 100. La técnica de distinción de las partes de una red y un equipo de la dirección IP se abordará más adelante.

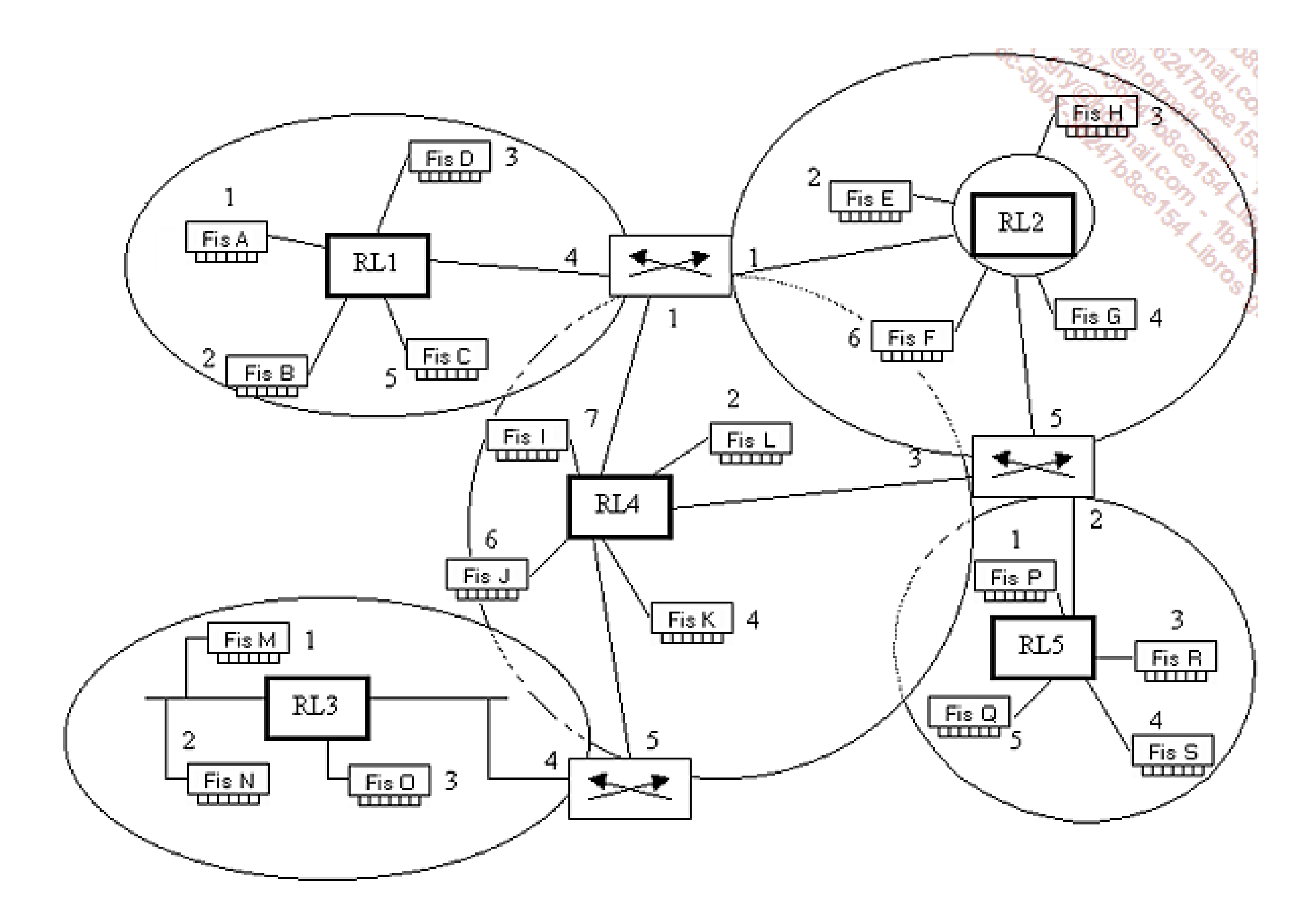
El concepto de red en 3 capas puede equivaler a una ciudad y sus calles. A cada elemento que deba ser identificado se le asigna un número, como a las puertas de los edificios de una calle.



Nivel 3: analogía de las redes lógicas y los nombres de las calles

Así, cuando alguien desee dirigirse a un destinatario cuya dirección conoce, primero se dirige hacia la calle y luego busca el número de puerta. Por ejemplo, si una persona, saliendo del número 2 de la Calle de las Lilas, desea encontrar a otra persona que vive en el número 4 de la calle de los Robles, se irá acercando progresivamente, preguntando el camino en cada intersección de calles. Cuando llegue a la calle correcta, solo le queda encontrar el número de la puerta.

Desde el punto de vista de una red, todas las redes lógicas están identificadas (corresponden a las calles). Y en cada una de ellas se numeran los componentes (identificación de los equipos).



Nivel 3: asignación de redes lógicas e identificadores de equipos

Los componentes de red que se deben identificar son las tarjetas de red de los ordenadores, las impresoras con interfaz de red, los routers (nivel 3 OSI), los módems.

c. La salida de una red lógica

Hemos decidido aclarar un poco este punto de vista antes de centrarnos en las explicaciones de la red TCP/IP, principal modelo basado en capas que realmente se utiliza. Por este motivo, vamos a hablar ahora de un concepto fundamental: el paso de una calle a otra en las intersecciones (transferencia de una red lógica a otra) se realiza a través de puertas de enlace. De manera predeterminada, la puerta de enlace representa el medio de salida de la calle, o de la red lógica.

Esta información se debe especificar en cada uno de los equipos de la subred, ya que de lo contrario no habría ninguna salida.

Además de la dirección lógica asignada a cada uno, que comprende una parte que califica a la subred y otra para el equipo, puede ser necesario indicar los datos de la puerta de enlace predeterminada. Este componente también puede ser denominado router.

Al igual que una calle puede tener varias intersecciones (si no es un callejón sin salida), una subred puede tener varias puertas de enlace. Veremos este caso a continuación.

En el nivel 3, hablamos de paquete IP para identificar la información transportada en este nivel. Atención, se habla también de paquete con UDP (capa 4), pero de segmento con TCP (capa 4).

Por ejemplo, para la red RL1 que tiene los hosts A, B, C, D, la información de configuración será la siguiente:

Equipo	Dirección MAC	Dirección lógica	Puerta de enlace

A	FisA	(RL1,1)	(RL1,4)
B	FisB	(RL1,2)	(RL1,4)
C	FisC	(RL1,5)	(RL1,4)
D	FisD	(RL1,3)	(RL1,4)

La salida de la red RL2, que tiene los equipos E, F, G y H, se hace por la puerta de enlace (RL2,1) o por la (RL2,5). Es necesario, por tanto, elegir.

Para ello podemos dar prioridad a la dirección más probable. Por ejemplo, si los puestos de red RL2 son susceptibles de querer ir a RL1, la utilización de la puerta de enlace (RL2,1) es la más lógica. Esta reflexión se puede efectuar para cada caso.

De esta manera, para los equipos de RL2, las puertas de enlace podrían ser las siguientes. Vea que este tipo de configuración permite repartir la carga entre las puertas de enlace.

Equipo	Dirección MAC	Dirección lógica	Puerta de enlace
E	FisE	(RL2,2)	(RL2,1)
F	FisF	(RL2,6)	(RL2,1)
G	FisG	(RL2,4)	(RL2,5)
H	FisH	(RL2,3)	(RL2,5)

d. La transmisión de paquetes en la intrarred

¿Cómo una trama emitida por una tarjeta de red lógica dada puede llegar finalmente a otra tarjeta de red situada en otra red lógica de la intrarred?

¿Cuáles son las etapas que se implementan?

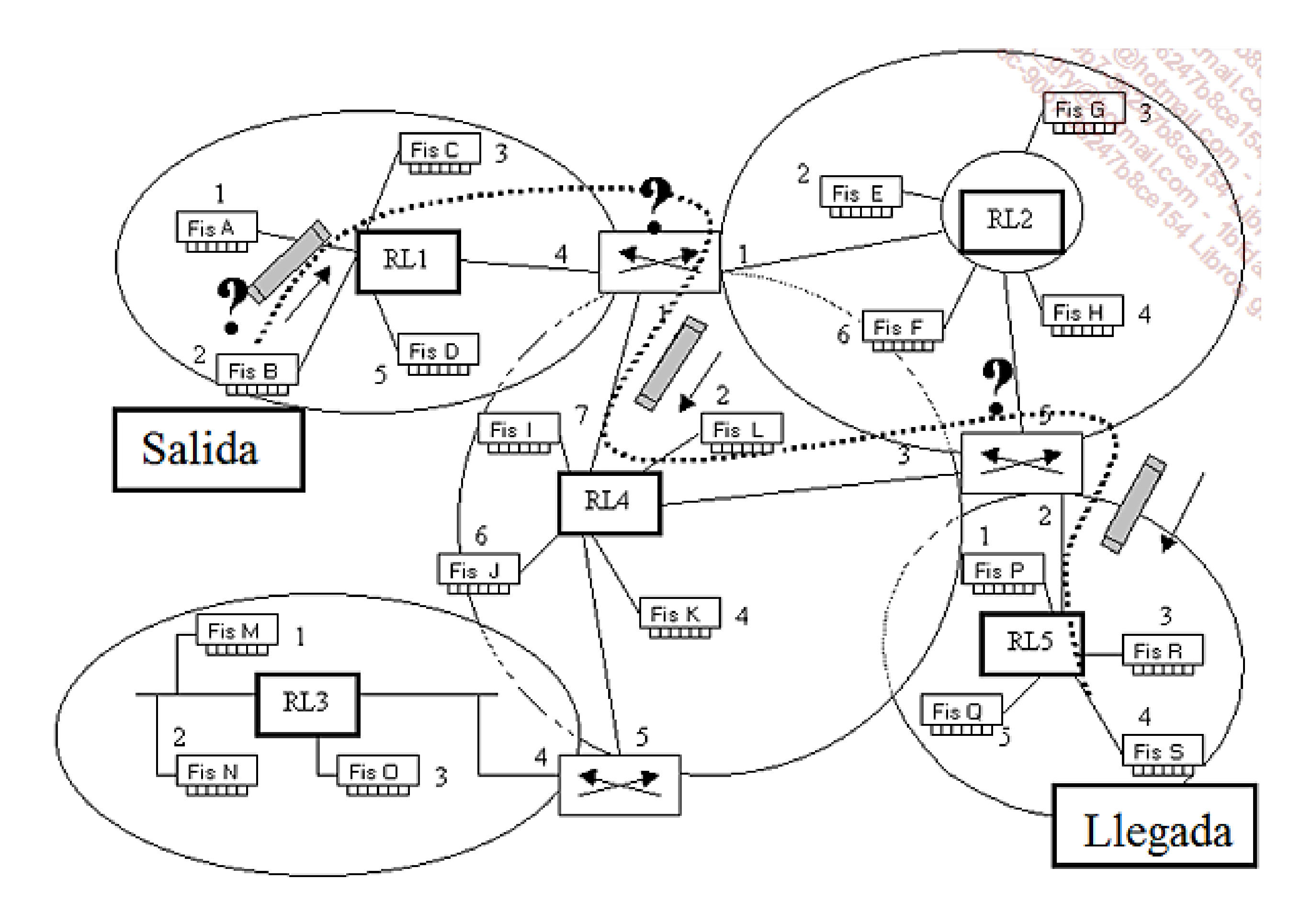
¿Qué mecanismos se ejecutan para que la tarjeta tome la decisión correcta que le permita, en primer término, salir de su red lógica y, a continuación, acercarse poco a poco a la red lógica del destinatario, hasta alcanzarlo finalmente?

Consideremos que un equipo intenta enviar datos a otro mediante tarjetas de red.

El emisor conoce su dirección lógica, que incluye la puerta de enlace. También ha obtenido la dirección completa del destinatario.

Se presentan dos casos:

- El emisor y el destinatario están en la misma red lógica.
- El destinatario pertenece a una red lógica distinta.



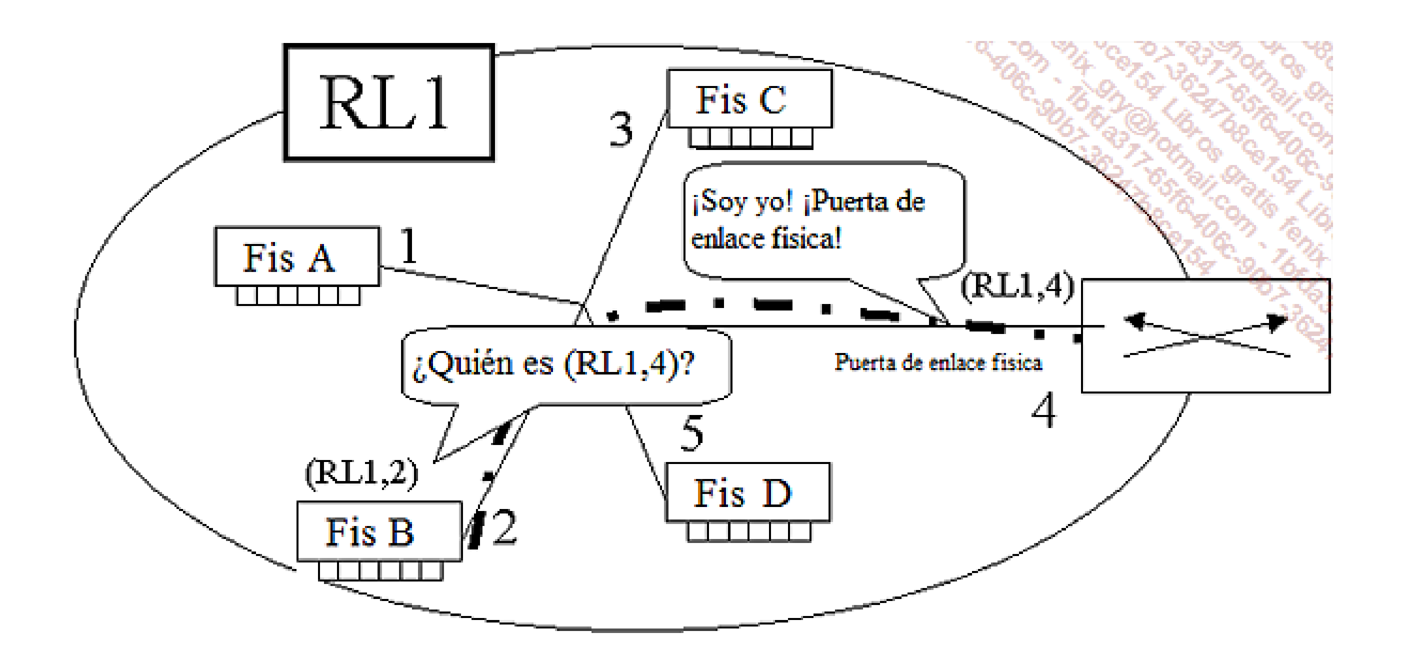
Nivel 3: propagación de un paquete en una intrarred

Caso 1: El emisor y el destinatario se encuentran en la misma subred

La comunicación aquí es de nivel 2, porque no es necesaria ninguna salida de la red lógica. El emisor obtiene esta información comparando su identificador de red con el de su interlocutor.

Para enviar realmente la trama al destino correcto, el emisor debe obtener la dirección física (MAC) de su interlocutor. Para ello envía primero una trama corta a todos los equipos de su red de nivel 2, sustituyendo la dirección física del destinatario por una dirección especial (por ejemplo, FF-FF-FF-FF-FF-FF), que significa que todo el mundo debe atender a la solicitud. Es aquí donde se plantea la pregunta: ¿quién me puede dar la dirección física correspondiente a esta dirección lógica? El equipo concerniente responde y envía la información solicitada.

En la siguiente ilustración se observa que esta solicitud se realiza a la puerta de enlace. La puerta de enlace se considera un equipo de la red y será la primera destinataria de los datos que deben salir.



Nivel 3: obtención de la dirección MAC de la puerta de enlace predeterminada

En realidad, el protocolo utilizado para obtener la dirección física a partir de una dirección lógica IPv4 en una red de nivel 2 es el *Address Resolution Protocol* (ARP).

Finalmente, el emisor está en condiciones de construir una trama que contenga, además de sus datos de direcciones física y lógica, la dirección del destinatario.

Caso 2: El emisor y el destinatario pertenecen a subredes distintas

Igual que en el caso anterior, se comparan los identificadores de red lógica. El equipo origen de la emisión constata que el suyo es distinto del de su interlocutor. La comunicación debe, por tanto, pasar un nivel y se busca una puerta de enlace en el nivel 3 del modelo OSI.

Este nodo de la red, que puede ser un router, es el que conoce la información de redirección de los datos comunicados y será utilizado como puerta de salida.

Si no se conoce, se realiza la búsqueda de la dirección física del router. En caso de respuesta positiva, se efectúa la transmisión hacia el destinatario. El emisor inicial se conforma con dirigir la información hacia la salida de la red lógica. No le importa cuál sea el enrutamiento seguido hasta el nodo final de la red. La trama, convertida en paquetes, contiene asimismo la dirección lógica de este destinatario final.

e. Distribución de paquetes en el router

Principios

Ya hemos visto que, si hay que realizar un tratamiento de nivel 3 (distintos identificadores de emisor y de destinatario), el router se convierte en el primer destinatario de los paquetes. Al recibirlos, el router sabe que los paquetes no son para él.

Por lo tanto, extrae el identificador de subred del destinatario final y consulta su tabla de transporte. Esta contiene la información de distribución hacia el destinatario final o hacia el próximo router.

Caso 1: El router puede dirigirse directamente al destinatario final

El router constata que una de las interfaces de red está declarada en la misma red lógica que el equipo final. Se conforma con construir un nuevo paquete de datos y enviarlo.

Caso 2: El router no puede alcanzar la red lógica del destinatario final

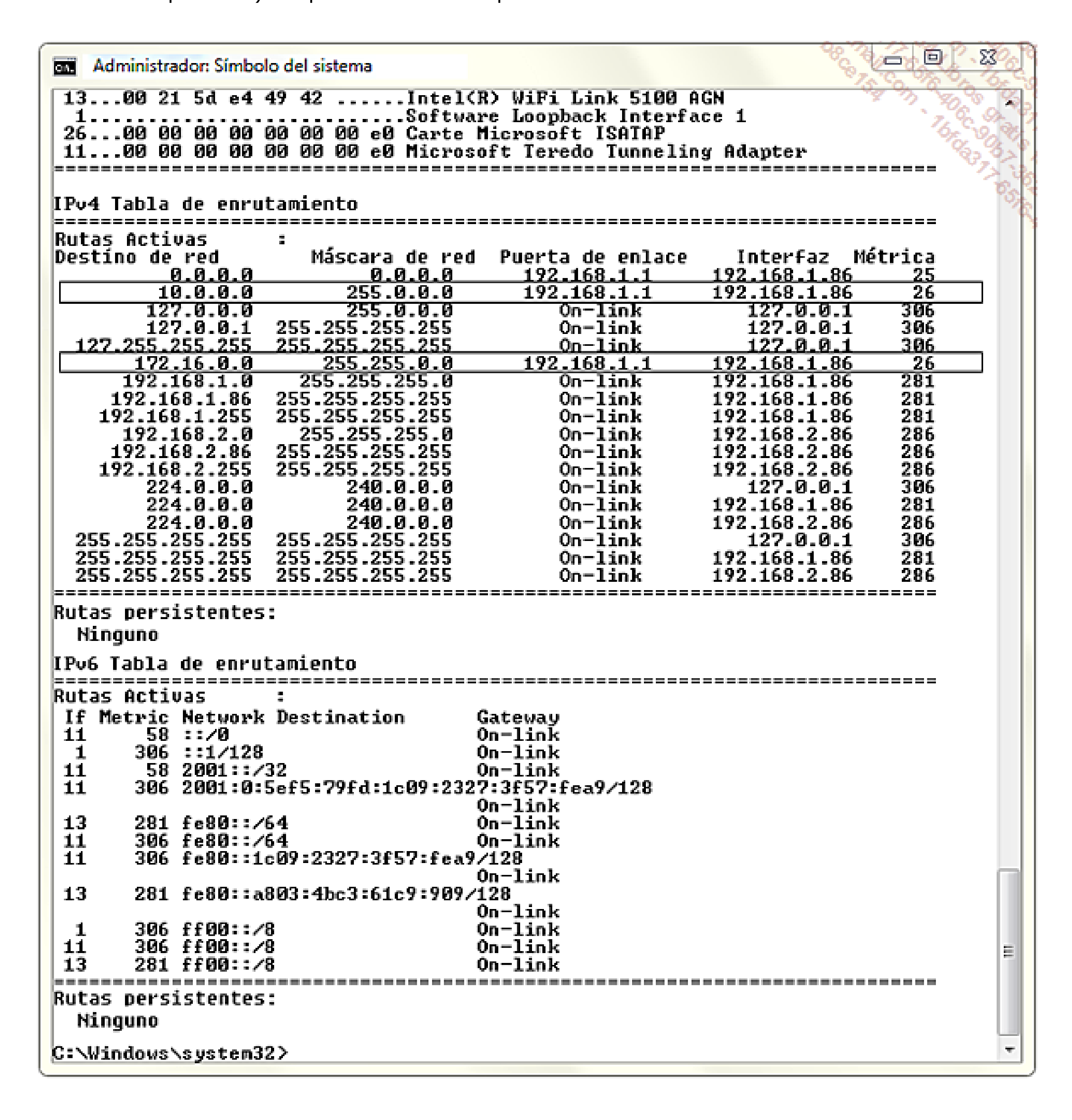
Si la tabla de transporte no contiene información de enrutamiento hacia la red lógica del destinatario, el router pone fin a la comunicación. El emisor recibe un mensaje que indica la imposibilidad de comunicarse con el destinatario solicitado.

Caso 3: El router puede alcanzar la red lógica del destinatario final

En este caso, se encuentra un camino en la tabla de transporte. Designa la dirección lógica (IP) del próximo router que permite acercarse a la red lógica de destino.

En la siguiente tabla de enrutamiento, vemos que el router dispone de dos interfaces con direcciones lógicas 192.168.1.86 y 192.168.2.86. Más adelante hablaremos de la dirección lógica 127.0.0.1, dirección de bucle local designada en todos los servicios.

Se han creado dos rutas hacia los destinos de red lógica 10. y 172.16 (destacadas con un recuadro en la pantalla). La puerta de enlace para comunicarse con estas redes es 192.168.1.1.



```
Administrador: Símbolo del sistema
 13...00 21 5d e4 49 42 ......Intel(R) WiFi Link 5100 AGN
  1...........................Software Loopback Interface 1
 26...00 00 00 00 00 00 00 e0 Carte Microsoft ISATAP
 11...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
===========================================================================

IPv4 Tabla de enrutamiento
===========================================================================
Rutas Activas       :
Destino de red        Máscara de red   Puerta de enlace    Interfaz  Métrica
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.86     25
         10.0.0.0        255.0.0.0      192.168.1.1    192.168.1.86     26
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    306
       172.16.0.0      255.255.0.0      192.168.1.1    192.168.1.86     26
      192.168.1.0    255.255.255.0         On-link     192.168.1.86    281
     192.168.1.86  255.255.255.255         On-link     192.168.1.86    281
    192.168.1.255  255.255.255.255         On-link     192.168.1.86    281
      192.168.2.0    255.255.255.0         On-link     192.168.2.86    286
     192.168.2.86  255.255.255.255         On-link     192.168.2.86    286
    192.168.2.255  255.255.255.255         On-link     192.168.2.86    286
        224.0.0.0        240.0.0.0         On-link        127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     192.168.1.86    281
        224.0.0.0        240.0.0.0         On-link     192.168.2.86    286
  255.255.255.255  255.255.255.255         On-link        127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     192.168.1.86    281
  255.255.255.255  255.255.255.255         On-link     192.168.2.86    286
===========================================================================
Rutas persistentes:
  Ninguno

IPv6 Tabla de enrutamiento
===========================================================================
Rutas Activas       :
 If Metric Network Destination      Gateway
 11     58 ::/0                     On-link
  1    306 ::1/128                  On-link
 11     58 2001::/32                On-link
 11    306 2001:0:5ef5:79fd:1c09:2327:3f57:fea9/128
                                    On-link
 13    281 fe80::/64                On-link
 11    306 fe80::/64                On-link
 11    306 fe80::1c09:2327:3f57:fea9/128
                                    On-link
 13    281 fe80::a803:4bc3:61c9:909/128
                                    On-link
  1    306 ff00::/8                 On-link
 11    306 ff00::/8                 On-link
 13    281 ff00::/8                 On-link
===========================================================================
Rutas persistentes:
  Ninguno

C:\Windows\system32>
```

Visualización de la tabla de enrutamiento de un ordenador con Windows

Tras obtener la información necesaria en su tabla de enrutamiento, el router solicita la dirección

física que corresponde a la puerta de enlace del destino (en el ejemplo anterior, la que corresponde al identificador lógico 192.168.1.1), si no la tenía ya.

A continuación crea una nueva trama destinada a ese interlocutor, pero que contiene los datos del equipo final.

El enrutamiento por salto continuará de la misma manera.

Si una tabla de enrutamiento no incluye directamente la información de distribución hacia la subred final, puede contener un itinerario predeterminado. Este itinerario se utiliza de forma sistemática, lo que evita el caso número 2.

4. Nivel 4 - capa de Transporte

En el modelo OSI, esta es la cuarta capa. Constituye la tercera dentro del protocolo TCP/IP, y con los mismos usos. Los niveles 3 y 4 a veces se agrupan bajo el nombre de capas medias.

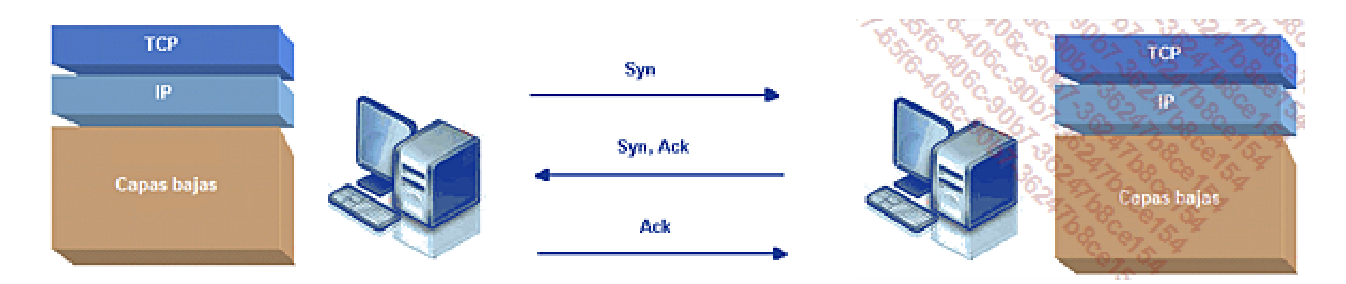
Las aplicaciones de tipo cliente/servidor que utilizan TCP/IP pueden emplear dos modos de transporte:

- conectado gracias al *Transmission Control Protocol* (TCP);
- no conectado, o paquete, con el *User Datagram Protocol*(UDP).

a. El modo conectado TCP

La primera elección consiste en la elaboración de un modo conectado que permita ejecutar un intercambio de información en bruto (grupo no formateado de bytes).

Se ejecuta un mecanismo para establecer una conexión TCP: se trata del 3 Way Handshake o intercambio en tres fases. Durante el proceso, se intercambian tres tramas:



Establecimiento de una conexión TCP en tres fases: 3 Way Handshake

Durante estos tres intercambios, el emisor y el destinatario se ponen de acuerdo sobre el tamaño de los *buffers* que se utilizarán para emitir y recibir los segmentos TCP intercambiados. Por ejemplo, si el emisor y el destinatario están en la misma red Ethernet 10/100 Mbps, el *buffer* acordado será de 12 x 1500 bytes, ya que 1500 bytes corresponden al tamaño de una trama en una red Ethernet. Lo llamamos *Maximum Transfer Unit* (MTU).

Además, en TCP, se ejecutan algunos acuses de recibo para permitir validar poco a poco el grupo entrante de bytes en bruto. El *buffer* se elige de modo que sea posible enviar varios segmentos simultáneamente, sin tener que esperar los acuses de recibo, lo que provocaría tiempos de espera perjudiciales para los intercambios de red. Así pues, los acuses de recibo procedentes del destinatario cruzarán a través de la red los segmentos TCP que posteriormente se validarán.

Vea a continuación un ejemplo de captura de esta fase inicial. El equipo 192.168.1.92 (detrás de un router ADSL) inicia una petición de conexión por el puerto 80 (Web) del servidor público 77.67.11.74 (servidor hotmail).

```
101 25.3831060 157.55.0.137   192.168.1.92   HTTP    887 HTTP/1.1 302 Found
104 25.5776810 192.168.1.92   157.55.0.137   TCP      54 51357 > http [ACK] Seq=3138 Ack=834 Win=16804 Len=0
105 25.7118050 192.168.1.92   77.67.11.74    TCP      66 51358 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=4 SACK_PERM=1
106 25.7523940 77.67.11.74    192.168.1.92   TCP      66 http > 51358 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1452 SACK_
107 25.7525680 192.168.1.92   77.67.11.74    TCP      54 51358 > http [ACK] Seq=1 Ack=1 Win=17640 Len=0
108 25.7645710 192.168.1.92   77.67.11.74    TCP    1314 [TCP segment of a reassembled PDU]
109 25.7649160 192.168.1.92   77.67.11.74    TCP    1314 [TCP segment of a reassembled PDU]
110 25.8212810 77.67.11.74    192.168.1.92   TCP      54 http > 51358 [ACK] Seq=1 Ack=1261 Win=17120 Len=0

⊞ Frame 108: 1314 bytes on wire (10512 bits), 1314 bytes captured (10512 bits) on interface 0
⊞ Ethernet II, Src: a0:88:b4:d9:4c:7c (a0:88:b4:d9:4c:7c), Dst: 00:25:15:21:f1:20 (00:25:15:21:f1:20)
⊞ Internet Protocol Version 4, Src: 192.168.1.92 (192.168.1.92), Dst: 77.67.11.74 (77.67.11.74)
⊞ Transmission Control Protocol, Src Port: 51358 (51358), Dst Port: http (80), Seq: 1, Ack: 1, Len: 1260
```

Captura de trama de establecimiento de una conexión TCP

Aquí se observa, en la trama 105, una petición de conexión [SYN] al puerto 80 del servidor a partir del cliente (puerto 51358). A continuación, el servidor responde [SYN, ACK] al cliente (trama 106). Finalmente, el cliente acusa recepción de la inicialización que ha pedido al servidor (trama 107).

b. El modo no conectado UDP

En contraposición, el modo UDP permitirá trabajar rápidamente en detrimento de la fiabilidad. El objetivo es, simplemente, que suba la información que procede de las tramas de red a la capa de aplicación.

No se envía ningún acuse de recibo, tampoco se ofrece ninguna conexión inicial del tipo 3 Way Handshake. UDP no agrega nada al paquete que se ha transportado por IP, acelerando así considerablemente los intercambios.

5. Nivel 5 y superiores

Las capas superiores constituyen una única capa de aplicación en TCP/IP que puede o no utilizar las conexiones establecidas (con el modo no conectado) y permitir, finalmente, que los procesos que se realizan en distintos ordenadores puedan comunicarse entre sí.

Un *socket* corresponde a un identificador de proceso en un entorno de red TCP/IP.

El identificador de *socket* está compuesto por la dirección IP, el protocolo de capa 4 OSI utilizado (TCP o UDP), así como por un número de puerto (TCP o UDP). Este número de puerto está comprendido entre 0 y 65535.

Socket = dirección IP:TCP o UDP:número de puerto

Por ejemplo, un *socket* servidor HTTP sería 192.168.2.200:TCP:80.

Al cliente se le asigna dinámicamente el socket para permitir una comunicación fluida en los dos sentidos.

Observe que, a partir de Windows Vista, los puertos aleatorios que se utilizan están entre 49152 y 65535. Las versiones anteriores de Windows utilizan números de puerto aleatorios superiores a 1024.

Una vez establecida la conexión TCP, puede comenzar el intercambio de información entre el cliente y el servidor.

Estándares y organismos

En esta sección, describiremos los principales organismos de estandarización en cuanto a redes y daremos algunos ejemplos de implementación.

1. Tipos de estándares

Se distinguen los estándares legales, *de jure*, de los estándares impuestos por un fabricante, *de facto*, cuya utilización está muy extendida.

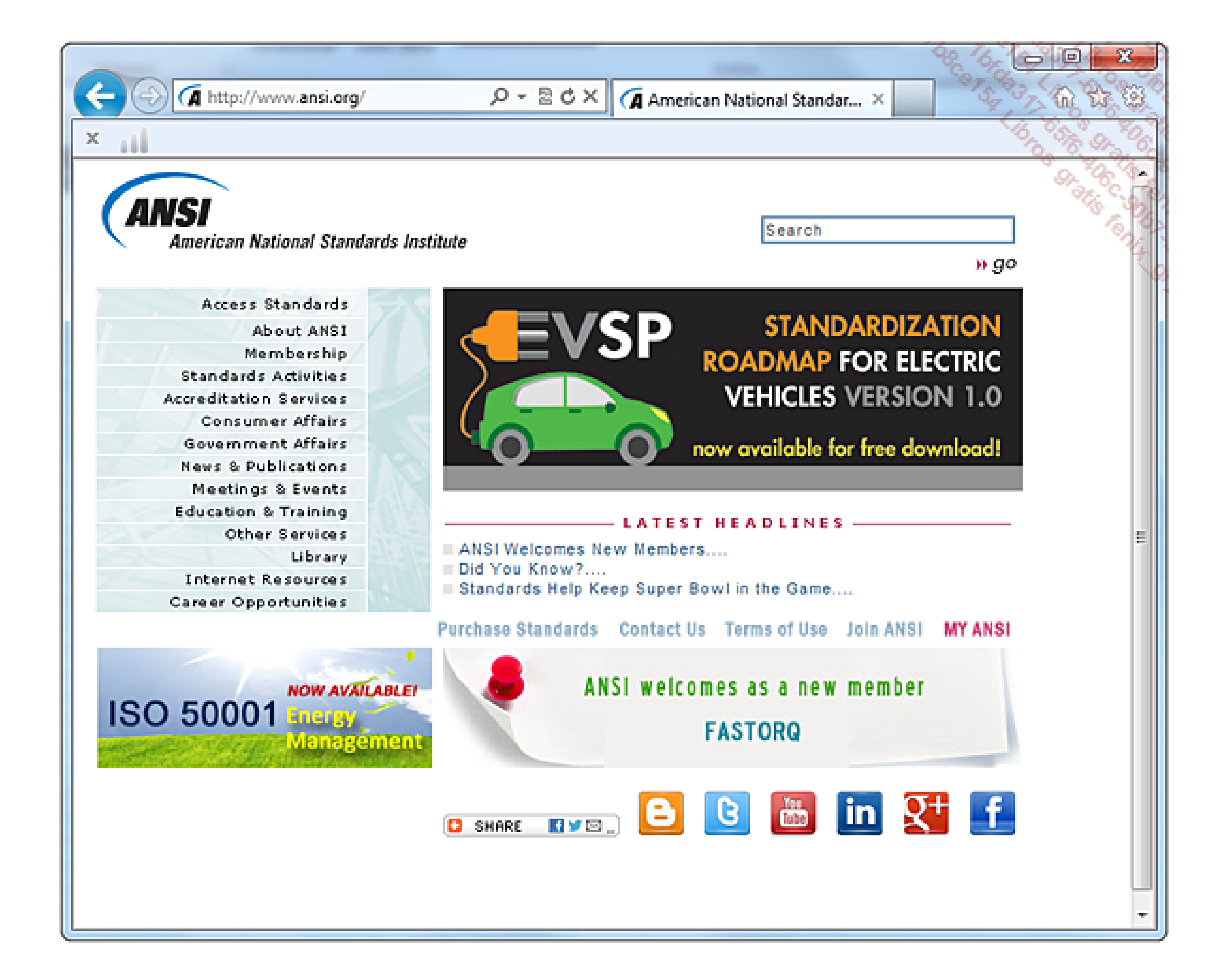
Además, calificaremos como propietario a un tipo de estándar inventado y controlado por una empresa, y no propietario a un estándar desarrollado por un organismo de estandarización.

2. Algunos organismos de estandarización para redes

No existe una única fuente de estándares. Por regla general, un organismo de estandarización coordina las especificaciones de distintas soluciones de hardware o software. Entre estos organismos, estamos ligados a los que elaboran la mayoría de los estándares para redes locales e internacionales. Cada organismo desarrolla una parte diferente de la actividad de las redes.

a. American National Standards Institute (ANSI)

Se trata de un organismo creado por empresarios e industriales norteamericanos, que se dedica al desarrollo de estándares en cuando al comercio y las comunicaciones. ANSI trabaja esencialmente en las codificaciones, los alfabetos, los modos de indicación, los lenguajes de programación, la interfaz SCSI, etc.



Sitio Web: www.ansi.org

ANSI representa a los EE.UU. en la ISO.

Ejemplos de implementación:

- ANSI/IEEE 802.3: *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD).
- ANSI X3.135: estandarización de *Structured Query Language* (SQL).
- ANSI X3T9.5: especificaciones para *Fiber Distributed Data Interface* (FDDI).
- Estandarización para el transporte en los lenguajes FORTRAN, COBOL, C.

b. Unión internacional de las telecomunicaciones (UIT)

El Comité Consultivo Internacional Telegráfico y Telefónico (CCITT) dejó su lugar a la Unión Internacional de las Telecomunicaciones (UIT), en inglés *International Telecommunication Union* (ITU).



Sitio Web: www.itu.int

Este comité estudia y recomienda la utilización de estándares de comunicación reconocidos en todo el mundo y publica sus recomendaciones cada cuatro años.

Sus protocolos se aplican a los módems, a las redes y a la transmisión por fax.

Cuenta con quince grupos de trabajo (de A a U). Cada uno de ellos desarrolla normas para cada materia diferente. Por ejemplo:

- T para el fax.
- V para las telecomunicaciones.
- X para las redes...

Ejemplos de implementaciones

Serie V

Las recomendaciones para la estandarización del diseño y el funcionamiento de los módems se llaman comúnmente serie V.

- V.32bis es el estándar de transmisión asíncrona y síncrona que llega hasta los 14400 baudios.
- V.42bis define las compresiones de datos del módem con el método Lempel Ziv.

Serie X

Esta serie se refiere a los estándares OSI.

- X.200 define el modelo de referencia OSI.
- X.25 especifica la interfaz de conmutación de los datos por paquetes.
- X.400 estandariza el tratamiento de mensajes (la mensajería electrónica).
- X.500 define la gestión de los directorios en un entorno distribuido.

c. Electronic Industries Alliance (EIA)

Esta asociación es un organismo que agrupa fabricantes norteamericanos de componentes y equipos electrónicos. Desarrolla estándares industriales para las interfaces entre el tratamiento de datos y los equipos de comunicación. Además, trabaja en estrecha colaboración con ANSI y UIT.

Ejemplo de implementación

RS-232, estándar para las conexiones serie con los conectores DB-9 o DB-25.

d. Institute of Electrical and Electronics Engineers (IEEE)

Uno de los principales institutos americanos de estandarización de las tecnologías de comunicación, el *Institute of Electrical and Electronics Engineers* (IEEE), nació de la fusión, en 1963, del *Institute of Radio Engineers* (IRE) y del *American Institute of Electrical Engineers*(AIEE). Este organismo, destinado a promover el conocimiento en la ingeniería eléctrica, es el que crea numerosos estándares ratificados por la ISO.

En esta organización, se coordinan personas en grupos de colaboración para trabajar sobre un tema específico y para ello forman un comité. Por ejemplo, el IEEE 1394 trabaja en los bus serie de tipo FireWire.

Los comités 802 deben su nombre a la fecha de inauguración, febrero de 1980. Son los que inician el desarrollo de estándares para redes en las capas bajas. Los distintos temas se reparten entre grupos de trabajo. Se puede citar, por ejemplo:

- 802.3, *Ethernet Working Group* (tipo LAN).
- 802.11, *Wireless LAN Working Group* (tipo WLAN).
- 802.15, *Wireless Personal Area Network* (tipo WPAN).
- 802.16, *Broadband Wireless Access Working Group* (tipo WMAN).



IEEE 802 LAN/MAN Standards Committee

IEEE 802 Working Group & Executive Committee Study Group Home Pages

Active Working Groups and Study Groups

- 802.1 Higher Layer LAN Protocols Working Group
  - Link Security Executive Committee Study Group is now part of 802.1
- 802.3 Ethernet Working Group
- 802.11 Wireless LAN Working Group
- 802.15 Wireless Personal Area Network (WPAN) Working Group
- 802.16 Broadband Wireless Access Working Group
- 802.17 Resilient Packet Ring Working Group
- 802.18 Radio Regulatory TAG
- 802.19 Wireless Coexistence Working Group
- 802.20 Mobile Broadband Wireless Access (MBWA) Working Group
- 802.21 Media Independent Handover Services Working Group
- 802.22 Wireless Regional Area Networks
- 802.23 Emergency Services Working Group

Inactive Working Groups and Study Groups

- 802.2 Logical Link Control Working Group

Disbanded Working Groups and Study Groups

- 802.4 Token Bus Working Group (material no longer available on this web site)
- 802.5 Token Ring Working Group
- 802.6 Metropolitan Area Network Working Group (material no longer available on this web site)
- 802.7 Broadband TAG (material no longer available on this web site)
- 802.8 Fiber Optic TAG (material no longer available on this web site)
- 802.9 Integrated Services LAN Working Group (material no longer available on this web site)
- 802.10 Security Working Group (material no longer available on this web site)
- 802.12 Demand Priority Working Group (material no longer available on this web site)
- 802.14 Cable Modem Working Group (material no longer available on this web site)

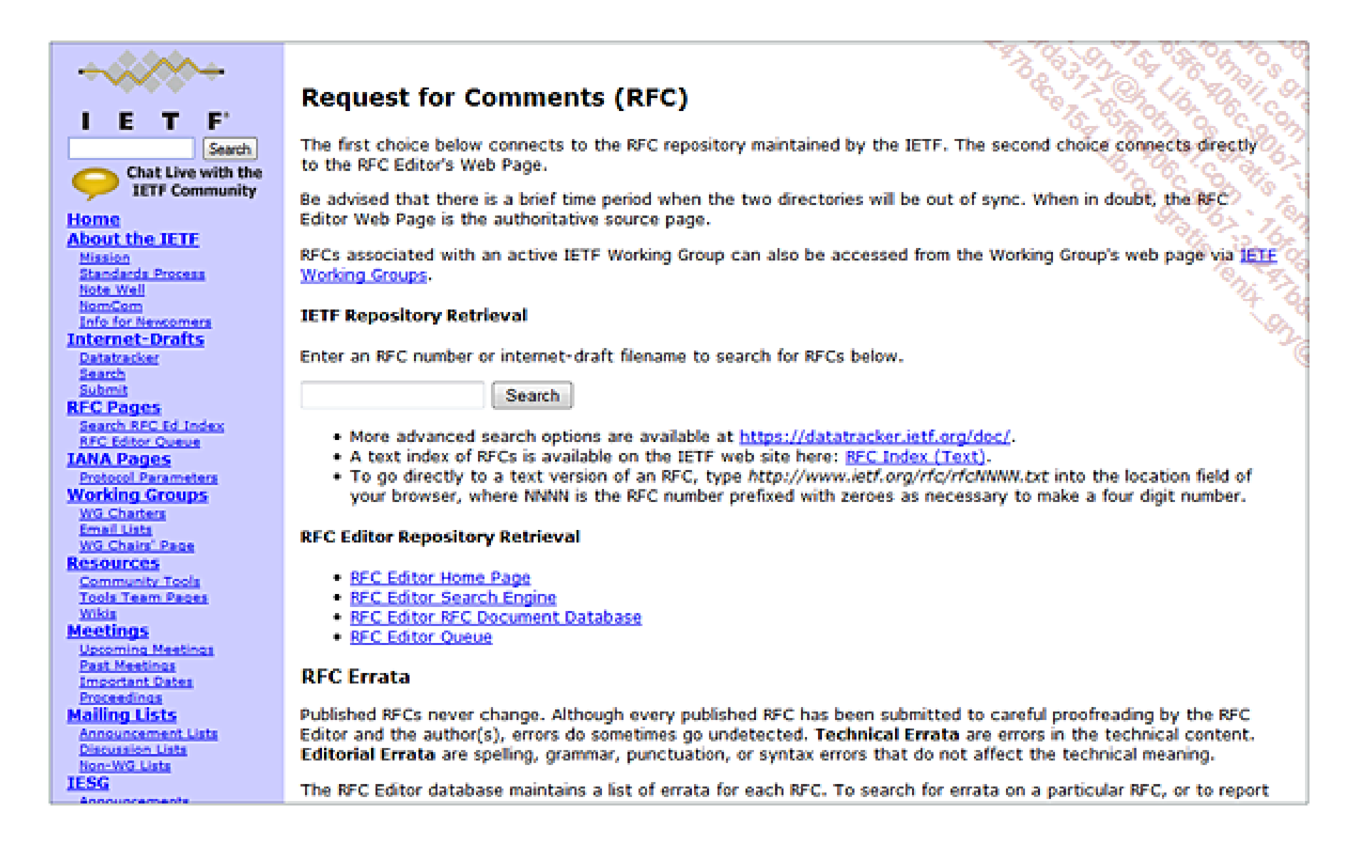
e. ISO

Especializada en el desarrollo y la normalización de estándares técnicos, ISO es una organización no gubernamental internacional. Agrupa a más de 150 países y su sede está en Ginebra, Suiza. Su nombre no es el acrónimo de *International Organization for Standardization*, que se podría traducir en castellano como Organización Internacional de Estandarización, sino que procede del griego «isos», que quiere decir igual.

f. Internet Engineering Task Force (IETF)

El objetivo del organismo *Internet Engineering Task Force* (IETF), miembro de la Internet Society, es el de mejorar el funcionamiento de la red Internet. Como en IEEE, hay grupos de trabajo que definen estándares, que se documentan en las publicaciones *Request For Comments* (RFC).

Una RFC está identificada por un número único. Cada desarrollo es objeto de una nueva documentación que puede completar o dejar obsoleta a la anterior. No hay actualización de RFC.



Sitio Web: www.ietf.org/rfc.html

Papel de una interfaz de red

Inicialmente vamos a examinar los parámetros que permiten configurar los periféricos de un PC y más concretamente una tarjeta de red.

1. Principios

La interfaz de red tiene el papel de intermediario entre el ordenador y el soporte de transmisión. Puede ser un pequeño componente soldado a la placa base o una tarjeta de red (NIC - *Network Interface Card*) independiente. En este último caso se instala en una ranura de expansión (*slot*). Su papel es preparar los datos que deben transmitirse antes de enviarlos e interpretar los recibidos. Para ello, contiene un transmisor-receptor.

El controlador (*driver*) del periférico se encarga del vínculo entre la tarjeta y el sistema operativo. Este componente informático corresponde a la capa de Conexión de datos del modelo OSI.

2. Preparación de los datos

La capa física prepara los datos (bits) que deben transmitirse en forma de señales. Los intercambios entre el ordenador y la tarjeta se efectúan en paralelo mediante el bus de la máquina. La tarjeta de red ordenará la información en series antes de transmitir las señales a través del soporte físico.



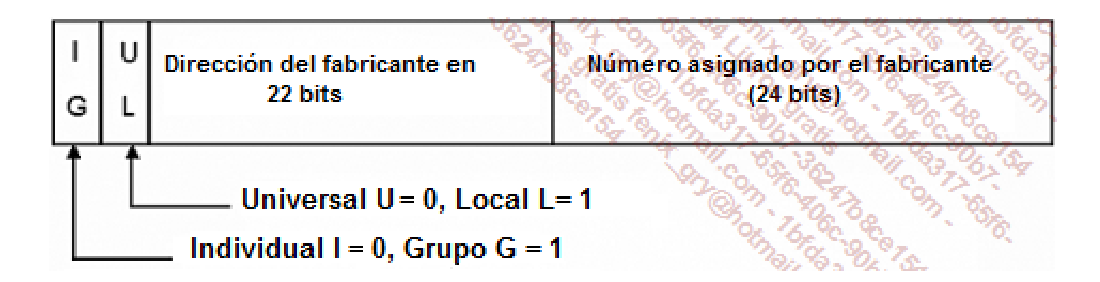
Opciones y parámetros de configuración

Cualquier punto de entrada/salida en una red debe definirse para que la trama sea recibida (aceptada) por el periférico adecuado. Una tarjeta de red o un puerto de serie deben tener un número que permita ubicarlos en el nivel más bajo (del modelo OSI).

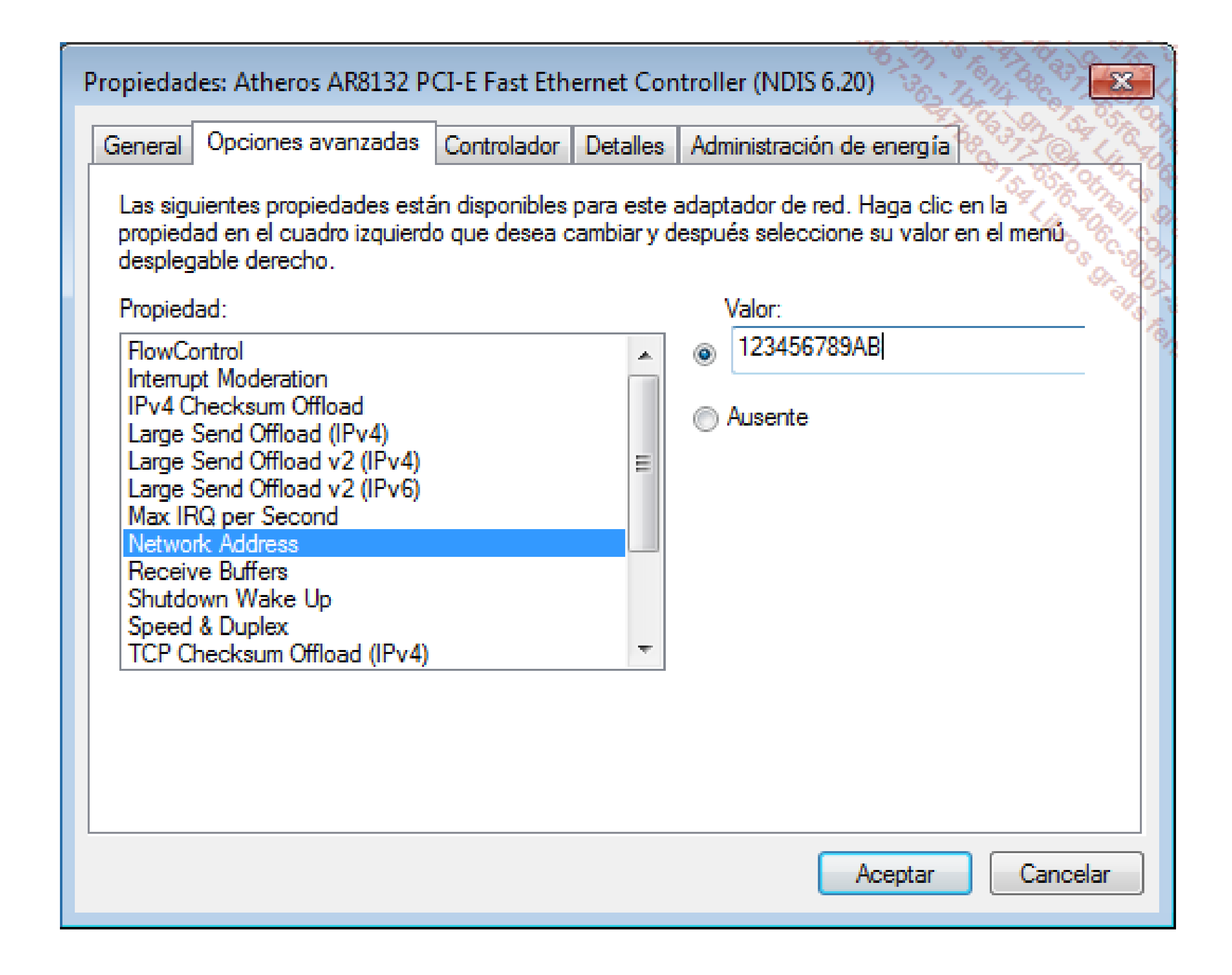
1. Dirección física

Es una dirección física de seis bytes que permite identificar la interfaz de red en una red local de tipo Ethernet (la más frecuente y que trataremos más adelante). El IEEE asigna los tres primeros bytes de esta dirección para identificar el fabricante del hardware (p. ej., 00AA00 para el fabricante Intel y 00A024 para 3Com). Los tres bytes restantes se dejan a disposición del fabricante, que debe combinarlos en las tarjetas de tal manera que ninguna tenga la misma dirección física en una red de nivel 2.

Una dirección MAC puede identificar una tarjeta de red única (I = 0) o una asociada a un grupo de tarjetas (G = 1). Esta dirección puede ser única globalmente (U = 0) o simplemente única en un perímetro limitado (L = 1).



Teóricamente, nada impide al sistema operativo trabajar con direcciones físicas diferentes de las del fabricante. Por ejemplo, en Windows, al acceder a las Propiedades de la tarjeta de red, podemos configurar una nueva dirección física diferente de la asignada por defecto. Basta con validar para que la nueva dirección MAC se haga efectiva inmediatamente.



Visualización de opciones avanzadas de una tarjeta de red en Windows

El comando **ipconfig /all** en Windows o **ifconfig -a** en Unix/Linux permite comprobarlo.

Esta dirección se utiliza cada vez que un equipo, o más bien su tarjeta de red, tiene que emitir una trama hacia otra tarjeta de red. Es posible, sin embargo, enviar un paquete no a una, sino a varias tarjetas sustituyendo la dirección única del destinatario por una dirección múltiple (a menudo una dirección de difusión, que se representa como *FFFFFFFFFFFF*, es decir, todos los bits de los seis bytes a 1).

Así, cada dirección que se refiera a varios equipos verá reforzado su bit más significativo (el de la izquierda) con '1' (p. ej., FFFFFF.FFFFFF), con '0' en el caso contrario (p. ej., 00AA00.123456).

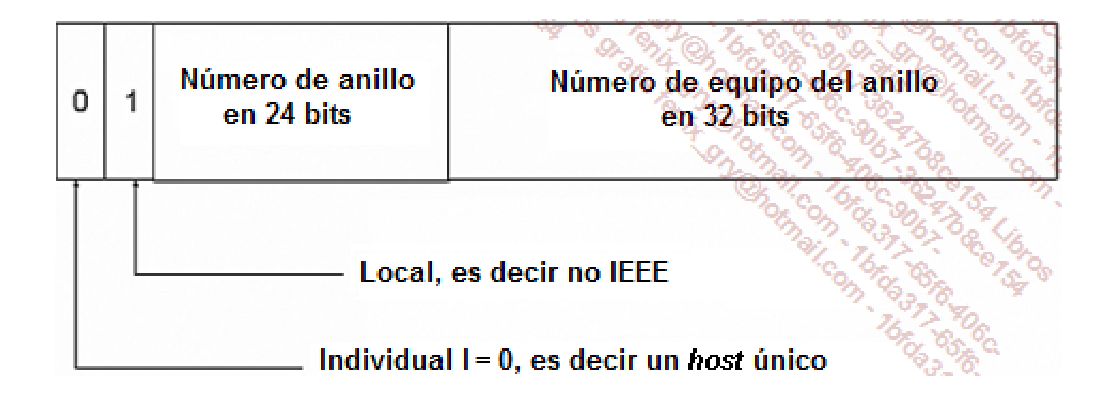
Por ejemplo, cuando una tarjeta de red efectúa una petición *Address Resolution Protocol* (ARP), envía una difusión en su red de nivel 2, es decir, el destinatario físico de la trama emitida es «todo el mundo», FF-FF-FF-FF-FF-FF, como se muestra a continuación:

```
+Frame: Base frame properties
-ETHERNET: ETYPE = 0x0806 : Protocol = ARP:  Address Resolution Protocol
  +ETHERNET: Destination address : FFFFFFFFFFFF
  +ETHERNET: Source address : 00A024B6132D
   ETHERNET: Frame Length : 60 (0x003C)
   ETHERNET: Ethernet Type : 0x0806 (ARP:  Address Resolution Protocol)
   ETHERNET: Ethernet Data: Number of data bytes remaining = 46 (0x002E)
-ARP_RARP: ARP: Request, Target IP: 172.17.0.3
   ARP_RARP: Hardware Type = Ethernet (10Mb)
   ARP_RARP: Protocol Type = 2048 (0x800)
   ARP_RARP: Hardware Address Length = 6 (0x6)
   ARP_RARP: Protocol Address Length = 4 (0x4)
   ARP_RARP: Opcode = Request
   ARP_RARP: Sender's Hardware Address = 00A024B6132D
   ARP_RARP: Sender's Protocol Address = 172.17.0.92
   ARP_RARP: Target's Hardware Address = 000000000000
   ARP_RARP: Target's Protocol Address = 172.17.0.3
   ARP_RARP: Frame Padding
```

Identificación de una dirección de difusión (niv. 2)

Una dirección que asigna IEEE reforzará el segundo bit significativo con '0', mientras que un valor '1' indicaría que la dirección corresponde a una dirección no normalizada.

Por ejemplo, en Token Ring, la dirección de un equipo se compone del siguiente modo:



Asignación de direcciones físicas Token Ring

Históricamente, era posible crear grupos en Token Ring (G = 1).

La lista completa de los prefijos de direcciones MAC asignados a los fabricantes (OUI - *Organizationally Unique Identifiers*) se puede consultar en la siguiente URL:http://standards.ieee.org/regauth/oui/index.shtml

2. Interrupción

Cualquier periférico del PC se conecta al microprocesador a través de una línea dedicada o línea de interrupción (IRQ - *Interrupt ReQuest*). Cuando el periférico necesita el microprocesador para trabajar, le envía una señal por esta línea (tensión eléctrica que pasa al estado bajo). En total existen 16 líneas de interrupción (2 x 8 líneas en cascada). Algunas líneas se asignan por defecto y otras están disponibles para recibir periféricos suplementarios. El microprocesador administra estas líneas por orden de prioridad: cuanto más bajo sea el número de la interrupción, más alta es su prioridad.

Gracias a la técnica Plug and Play, que permite la detección de la tarjeta y la asignación

automática de sus parámetros, ya no es tan necesario conocer esta información.

3. Dirección de entrada/salida

Los periféricos interrumpen al microprocesador cada vez que necesitan intercambiar información. Esta información es recibida o enviada por una puerta de entrada/salida localizada en una dirección particular: la dirección de entrada/salida. Esta dirección apunta hacia una gama de a lo sumo 32 bytes, que permitirá almacenar datos y, también, información que indica qué hacer con estos datos.

4. Dirección de memoria base

Es una dirección de memoria temporal cuyo papel consiste en hacer una especie de cojín (*buffer*) en la recepción o la emisión de la trama en la red.

Esta dirección tiene que ser un múltiplo de 16; por ello se escribe a menudo en hexadecimal sin el ’0’ final, que se da por sabido.

5. Canal Direct Memory Access (DMA)

En la mayoría de los casos, los periféricos dependen del microprocesador para transferir información desde su *buffer* hacia la memoria RAM o viceversa. Como vemos, existen periféricos que disponen de un canal particular para poder intercambiar directamente información con la memoria del PC, sin recurrir al microprocesador (en segundo plano).

Algunos periféricos, en particular las tarjetas de red, disponen de un canal DMA de 1 a 7.

6. Bus

Todos los datos intercambiados entre los periféricos y el ordenador pasan por un bus de datos. Durante mucho tiempo este intercambio se efectuaba sobre todo a través de vías paralelas y la velocidad de transmisión dependía mucho de su amplitud, por ejemplo 16, 32 o 64 bits. Las nuevas tecnologías de bus favorecen soluciones de transferencias en serie, en las que los bits se envían uno tras otro. Con el desarrollo de los medios, la velocidad se ha ido superando y los conectores son más pequeños.

Los buses históricos, *Industry Standard Architecture* (ISA), *Extended Industry Standard Architecture* (EISA) y *Micro Channel Architecture* (MCA), han dejado su lugar a otros más modernos.

El administrador de dispositivos de Windows permite obtener información precisa de la asignación de los recursos de hardware:

Visualización de las direcciones de memoria y de las IRQ

a. El bus Peripheral Component Interconnect (PCI)

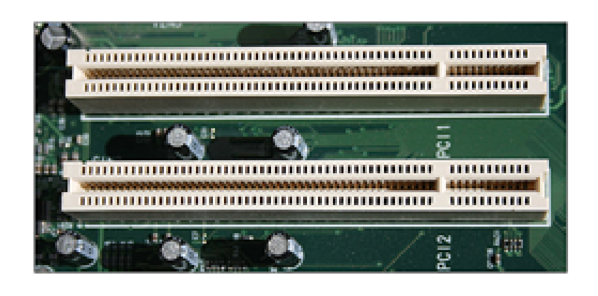
Este bus se convirtió en el estándar para las tarjetas de expansión. En el ordenador, el conector es blanco. Basándose al principio en una arquitectura de 32 bits en paralelo, se mejoró llegando a 64 bits. PCI es Plug and Play, no necesita configurar la tarjeta que se inserta.

El bus PCI paralelo se utiliza cada vez menos por su bajo rendimiento. Su sucesor en versión serie es *PCI Express* (PCI-E o PCIe), llamado anteriormente *Third Generation I/O* (3GIO). Está destinado a sustituir a los diferentes buses internos PCI y AGP (*Accelerated Graphic Port*).

Este último prácticamente ya no se utiliza, ya que ha sido superado por PCI-E, en el que se conectan las tarjetas gráficas.

Además de ocupar menos espacio en el ordenador que sus predecesores, PCI Express es claramente más rápido. Están disponibles diferentes versiones, de velocidad 1x a 2 Gbps hasta 32x (64 Gbps).

Vea a continuación dos *slots* PCI en una placa base de un ordenador:



Slots PCI

b. El bus PC Card

Este es un producto del consorcio *Personal Computer Memory Card International Association*(PCMCIA) y se suele conocer con este nombre.

Se trata de una arquitectura reciente que se desarrolla en tarjetas del tamaño de una tarjeta de crédito. El estándar es independiente del sistema operativo utilizado. Esta tarjetas también integran el hardware Plug and Play, que evita la configuración manual.

Existen también tarjetas Ethernet:



Tarjeta Ethernet PCMCIA

tarjetas Wi-Fi:



Tarjeta Wi-Fi PCMCIA

o tarjetas 3G en formato PCMCIA:



Tarjeta 3G PCMCIA

c. El bus USB

Este bus serie para dispositivos externos hizo su aparición hace 15 años. Poco a poco ha sustituido los conectores de teclado/ratón PS/2, Serie (COM) y paralelo (LPT). Entre los dispositivos puede encontrar interfaces de red externas.



Interfaz Ethernet para puerto USB

La velocidad ha evolucionado desde la primera versión:

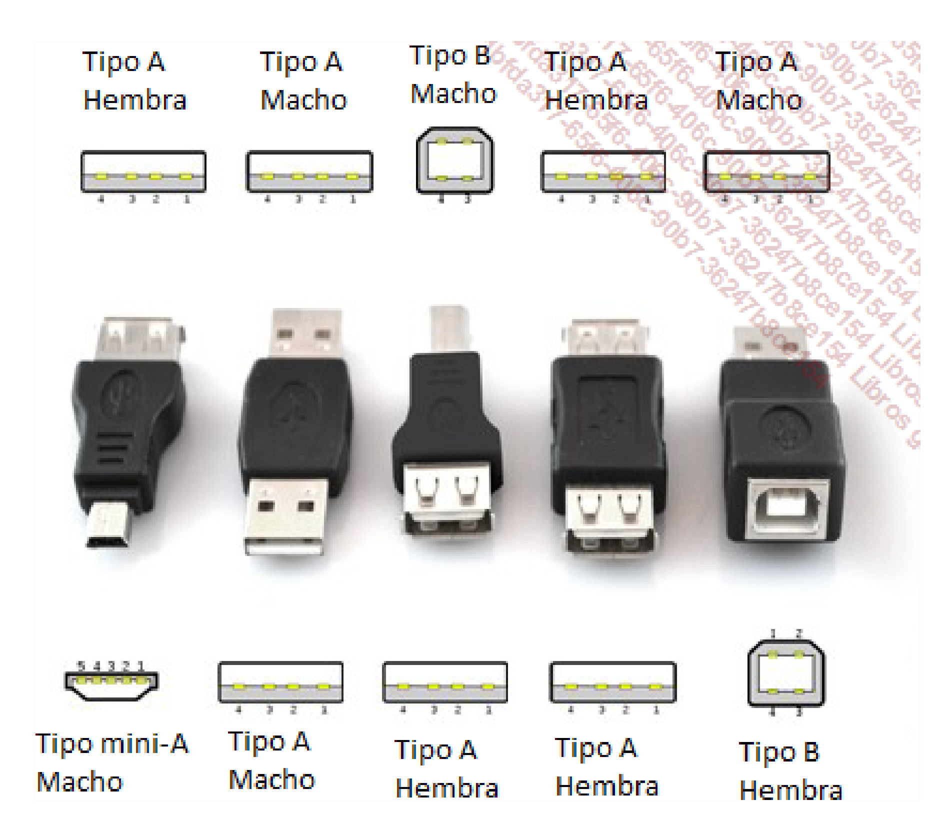
Versión	Denominación	Velocidad	Salida al mercado
1.0	Basic-speed	12 Mbps	1996
2.0	Hi-speed	480 Mbps	2000
3.0	SuperSpeed	5 Gbps	2009

Atención, a veces se habla de la velocidad en Mbps (Megabits por segundo) o Gbps (Gigabits por segundo); en este caso hay que dividir por 8 los valores expresados (ejemplo, 480 Mbps corresponden a 60 Mbps y 5 Gbps son 625 Mbps).

Observe que la versión 2.0 puede funcionar con la versión USB 1.0, pero con la velocidad de esta. Lo mismo ocurre con la versión 3.0 y la 2.0. Por el contrario, la versión 3.0 no puede funcionar con la versión 1.0.

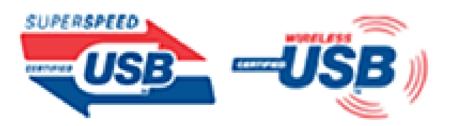
Existen dos tipos de conectores USB:

- El **conector de tipo A** es rectangular y permite conectar los dispositivos con un ancho de banda pequeño (por ejemplo, teclado, ratón, webcam).
- El **conector de tipo B**, cuadrado con dos biseles, destinado a conectar dispositivos de un ancho de banda grande (como los discos duros).



Conectores USB

Existen diferentes logos que permiten identificar la velocidad asociada a un dispositivo:









Logos USB

Es posible utilizar *hubs* USB para interconectar diferentes dispositivos a un ordenador.



Mini hub USB

Observe que, en este caso, el protocolo utilizado para permitir a los dispositivos acceder al soporte es un protocolo de tipo paso de testigo.

Los estándares y especificaciones están disponibles en la dirección:http://www.usb.org/developers/docs/

USB On-The-Go

Esta funcionalidad apareció desde la norma 2.0: se trata de permitir la conexión punto a punto entre dispositivos sin pasar por un huésped (p. ej., un ordenador). Un dispositivo OTG se puede conectar a otro dispositivo OTG, a un dispositivo no OTG o a un huésped.

En el caso de una conexión directa entre dispositivos OTG, la posición de la toma AB del cable permite saber cuál de los será el huésped.

De este modo, se pueden conectar fácilmente una cámara de fotos a una impresora, o un teléfono móvil a un lector MP3.



Ejemplo de dispositivo On-The-Go

d. El bus IEEE 1394

Este bus serie de alta velocidad es complementario al bus USB. Apareció en 1995.

También se llama **FireWire** (Apple), **i.Link** (Sony) o **Lynx** (Texas Instruments).

Este tipo de conectores también se pueden encontrar interna o externamente.

Las velocidades varían en función de los estándares.

Estos se expresan de la siguiente manera:

IEEE 1394x-S<velocidad-en-Mbps>

Donde x = a o b

Las velocidades teóricas varían de 100 a 3.200 Mbps:

Estándar IEEE	Denominación	Velocidad
1394a-S100	FireWire	100 Mbps
1394a-S200	FireWire	200 Mbps
1394a-S400	FireWire	400 Mbps
1394b-S800	FireWire 2 o FireWire Gigabit	800 Mbps
1394b-S1200	FireWire 2 o FireWire Gigabit	1,2 Gbps
1394b-S1600	FireWire 2 o FireWire Gigabit	1,6 Gbps
1394b-S3200	FireWire 2 o FireWire Gigabit	3,2 Gbps

Existen conectores de 4, 6 y 9 pines que son estándares.

Vea a continuación un conector de 4 pines:



Conector FireWire

El siguiente logo permite identificar el hardware que implementa FireWire.



Logo FireWire

Observe que es posible utilizar un cable FireWire para conectar dos ordenadores en red.

7. Conectores de cable de red

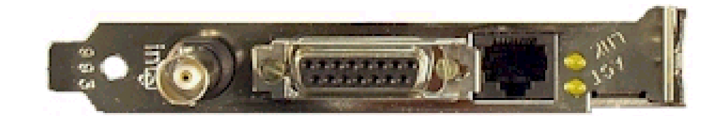
En una tarjeta de red por cable siempre hay por lo menos un conector para conectar el cable de transmisión. Los principales conectores son:

- RJ45 para el par trenzado (cobre).
- SC, ST, FC y LC para la fibra óptica.

a. El conector RJ45

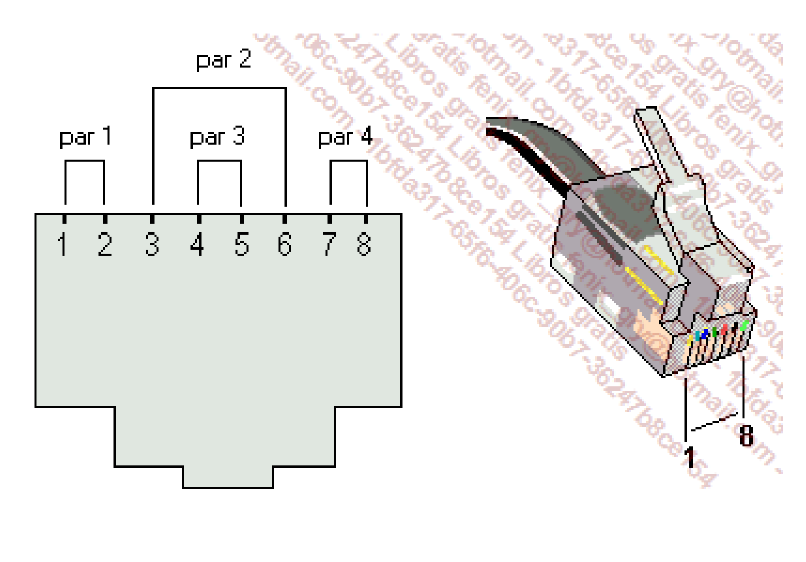
Durante mucho tiempo, las tarjetas ofrecían a la vez conectores BNC y RJ45. A veces, se añadía

una *Access Unit Interface* (AUI) para la conexión de un cable coaxial más grueso.



Conectores de red BNC, AUI y RJ45

El conector RJ45 es ahora, de largo, el más utilizado en las redes locales. También se utiliza en telefonía, en lugar del RJ11.



Pares de pines

Conector RJ45

b. El conector BNC

El cable coaxial fino conectado a un conector BNC fue durante bastante tiempo el soporte más utilizado para las redes locales. Todavía lo podemos ver en la industria.



Conector BNC

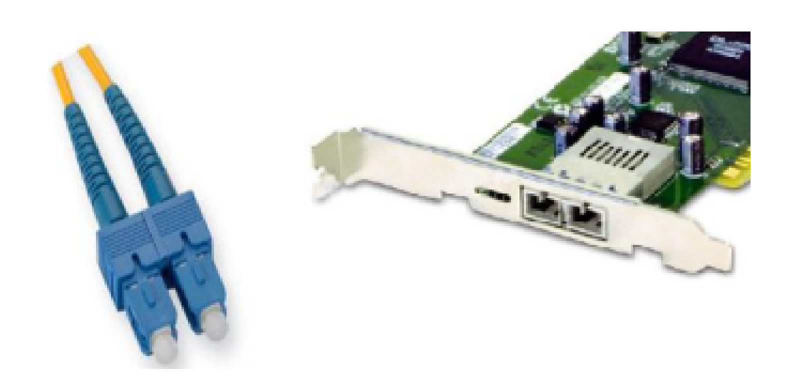
c. Los conectores de fibra óptica

La fibra óptica utiliza diferentes conectores que han evolucionado con el tiempo. El modelo ST, de forma redondeada y con bayoneta, tiende a desaparecer.



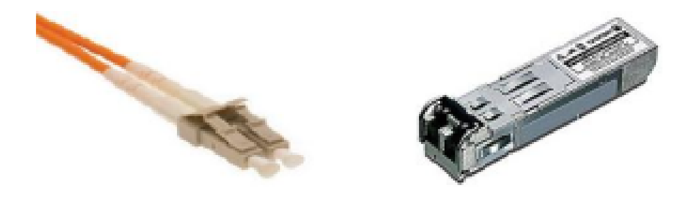
Conector de fibra óptica ST

Es más frecuente el uso del conector de cuerpo exterior cuadrado de tipo SC.



Conector SC y zócalo hembra correspondiente

Tiene la misma forma que el SC, pero el conector LC es mucho más pequeño. Se inspira en el conector RJ45. Se coloca fácilmente y ocupa poco espacio, de modo que permite una conexión doble, como su «hermano mayor» SC. Sobre la interfaz de red fija (por ejemplo, un conmutador), se coloca un mini-GBIC (*Gigabit Interface Converter*) que permite conectarlo.



Conector LC y mini-GBIC



Tarjeta de 4 puertos Fibre Channel - conectores LC

La conexión de fibra óptica, aunque simplificada a lo largo de los años, sigue siendo un punto delicado de la red y un tema para especialistas. Por ejemplo, los conectores anteriores no son apropiados para entornos en los que haya vibraciones. En este caso, se recomienda utilizar un conector FC. Este tiene forma redonda y se cierra mediante rosca, por lo que es más seguro y preciso.



Ejemplo de conector FC

En las redes metropolitanas, como la FDDI, se pueden utilizar conectores MIC dobles.



Conectores MIC dobles



GBIC

8. Velocidad

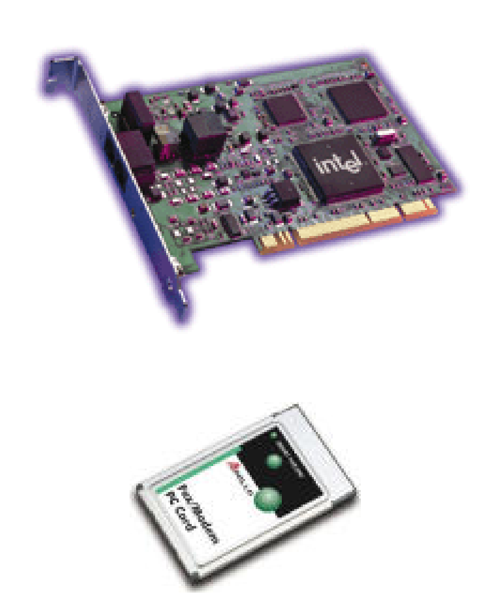
La unidad informática básica es el bit (*binary digit*), unidad binaria; por lo tanto, con dos combinaciones. Una sucesión de 8 bits forma un byte, que representa 256 combinaciones posibles.

La velocidad de transmisión de la información en una red es su flujo o ancho de banda. Se mide en múltiplos del número de bits por segundo.

Por ejemplo, los flujos más bajos son del orden de algunos miles, o kilo, bits por segundo (kbps o kbit/s). Si es más alta, la velocidad se mide en megabits por segundo (Mbps o Mbit/s) cuando es mil veces mayor, o en gigabits por segundo (Gbps o Gbit/s) cuando es un millón de veces más.

9. Otras interfaces de red

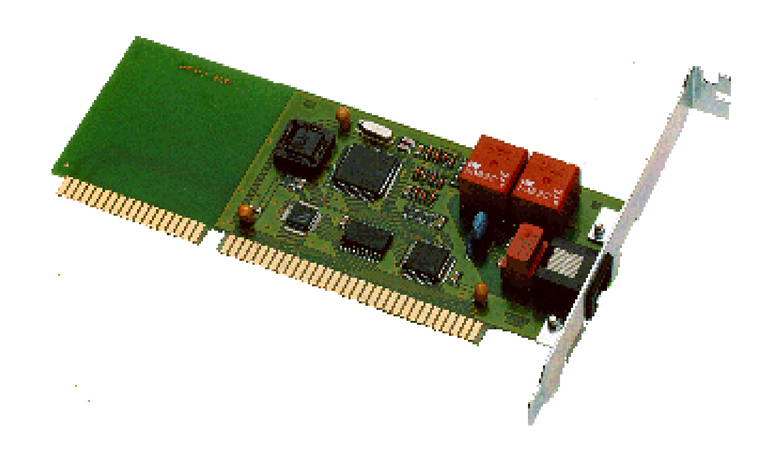
Las tarjetas de red no son los únicos medios de interconexión con una red informática. También están los módems internos o externos, que permiten hacer transferencias de datos a través de la Red Telefónica Conmutada (RTC). Existen los «clásicos», como Redes Digitales con integración de servicio (RDSI), o *Asymmetric Digital Subscriber Line* (ADSL) u otras. Más tarde volveremos a tratar estas tecnologías.



Tarjetas fax/módem

La tarjeta se parece a una tarjeta de red y dispone de un conector RJ45 que permite conectarla a la red telefónica mediante una interfaz S0.

El término anglosajón es ISDN (*Integrated Services Digital Network*).



Tarjeta ISDN

Es muy frecuente que una conexión ADSL funcione utilizando una tarjeta de red Ethernet 100 Mbps conectada a un módem ASDL o a un módem/router.



Módem ADSL

Existen también las tarjetas 3G, que se utilizan cada vez más:



Tarjeta 3G

Arranque desde la red

1. Principios

En algunos sitios, el sistema operativo de red, a nivel de las estaciones trabajo, se carga a partir de un programa escrito en memoria de solo lectura (PROM - *Programmable Read Only Memory*). Esto evita que las estaciones de trabajo deban tener obligatoriamente almacenamiento local (discos duros).

Esta solución garantiza que no tenga lugar ningún intercambio de información entre los puestos de trabajo. Así se obtiene una mayor confidencialidad de los datos de la empresa y al mismo tiempo se evita la introducción de virus.

La mayoría de las tarjetas de red disponen de un espacio para añadir un PROM de inicio. En el arranque, la tarjeta de red, que conoce su propia dirección física, envía una difusión (una trama dirigida a todo el mundo) que será reconocida por un servidor, que a su vez sabrá qué configuración de sistema operativo de red debe asociar a esta dirección.

2. Protocolos

Son varios los protocolos que posibilitan la inicialización a través de la red.

a. La conexión entre la dirección física y lógica

El protocolo *Address Resolution Protocol* (ARP) resuelve la dirección lógica IPv4 de nivel 3 en dirección lógica MAC de nivel 2.

La inversa, *Reverse Address Resolution Protocol* (RARP) permite, a través de la dirección física, determinar la dirección lógica. Así pues, en su inicialización (*bootstrap*), la estación de trabajo envía una petición RARP, con el fin de obtener una dirección IP correspondiente a la dirección MAC transmitida.

Una vez obtenida la dirección IP, el equipo también dispone de la dirección IP del servidor que respondió y entonces le pide un archivo a través del protocolo *Trivial FTP* (TFTP). Este archivo, de algunas decenas de KB, una vez descargado, se ejecutará y permitirá, finalmente, contactar con un servidor BOOTPARAM utilizando las llamadas a procedimientos remotos (RPC - *Remote Procedure Call*). La dirección IP del servidor se transmitirá, por último, al cliente, que a continuación descargará el sistema operativo a través de la red.

En IPv6, se utiliza el protocolo *Neighbor Discovery Protocol* (NDP) en lugar de ARP.

NDP realiza más funciones, como el descubrimiento de otros equipos situados en el mismo enlace, la determinación de su dirección, así como la identificación de los routers presentes.

Permite igualmente administrar la autoconfiguración de la dirección IPv6, sin servidor DHCP, o realizar la correspondencia entre la dirección IP y la dirección MAC.

Finalmente, entre las funciones de NDP, se encuentra *Duplicate Address Detection* (DAD), que permite garantizar que una dirección autoasignada sea única.

b. El protocolo BOOTP

Es una evolución de RARP y de BOOTPARAM, que permite la integración de otros parámetros, además de la dirección IP.

c. El protocolo DHCP

Finalmente, *Dynamic Host Configuration Protocol* (DHCP) es una evolución de BOOTP, en el sentido de que también permite al cliente enviar información al servidor. Por ejemplo, un cliente Windows actual será capaz de enviar su nombre DNS completo a un servidor DHCP.

Además, al contrario de lo que sucedía con BOOTP, que no administra la duración del proceso de asignación de parámetros TCP/IP, el protocolo DHCP es capaz de asociar parámetros durante un periodo de tiempo (hablaremos de concesión).

Existen diferentes soluciones de administración que a menudo conviven con la administración DNS: Microsoft, Linux, VitalQIP, Cisco Network Registrar.

El servicio DHCP se describe en el capítulo Protocolos de capas medias y altas de este libro.

d. PXE

Pre-boot eXecution Environment (PXE) se ejecuta completamente en la red y se ayuda de los protocolos DHCP y TFTP. Esta técnica se ha generalizado y la mayor parte de los ordenadores que incorporan interfaces de red integradas en la placa base permiten un arranque de este tipo. Para activarlo, basta con solicitar el arraque de red en el *setup* del ordenador.

Se han añadido otras características adicionales a las interfaces de red, como *Wake On LAN* (WOL), que permite iniciar un PC a distancia a través de la red, o el desarrollo propietario de Intel «vPro», que permite dirigir un PC remotamente.

Codificación de los datos

Hablamos de datos para precisar la información original que queremos intercambiar.

De todos modos, estos datos deben utilizar uno o más canales de comunicación para llegar a los destinatarios. Por ejemplo, la voz humana puede transmitirse a través del aire o de la red telefónica conmutada una vez digitalizada.

A continuación definimos como señal la información que transita por un canal de comunicación. El paso de un lado al otro a menudo implica diferentes etapas de transformación.

1. Tipos de datos y de señales

Distinguiremos los datos digitales de los datos analógicos. Del mismo modo, hablaremos de señal digital cuando su representación implique un número finito de estados (p. ej., tensiones cuadradas de amplitud 20 ms). Una señal analógica está representada por una onda sinusoidal que puede tomar un sinfín de valores.

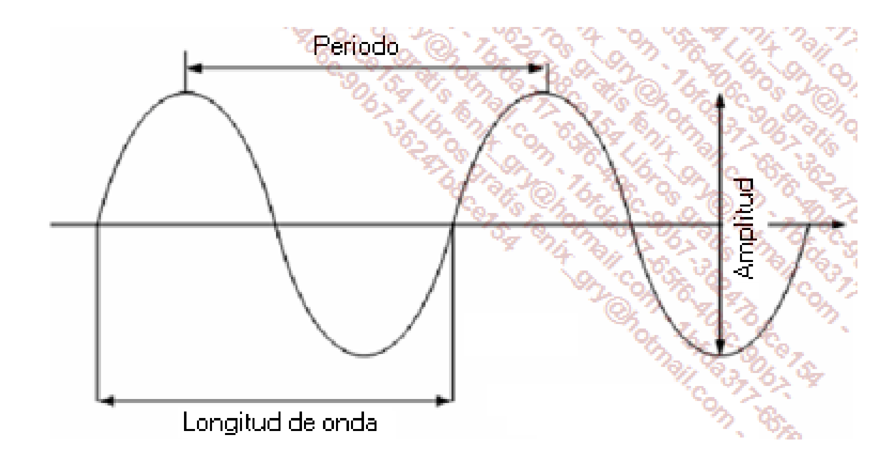
a. La señal analógica

Basta con lanzar una piedra al agua para constatar que una onda omnidireccional se propaga en forma de sinusoide. Los sonidos se propagan siguiendo los mismos principios, pero operando sobre variaciones de presión en el aire.

Este tipo de señal es fácilmente reproducible incluso en soportes limitados (físicos, por ejemplo cables).

Una onda es una señal analógica periódica. Su primera característica es la frecuencia, cuya medida de unidad es el hertz (Hz), y que representa el número de oscilaciones por segundo.

El periodo designa la duración de una oscilación completa en segundos. El periodo es inverso a la frecuencia. Se puede calcular también la longitud de onda, distancia en metros recorrida por una oscilación. La altura de la onda se designa como amplitud. La fase indica el sentido de la onda.



b. La señal digital

Este tipo de señal, que se basa en la sincronización por señal de reloj, permite codificar la información haciendo variar la amplitud.

La velocidad de estas señales se expresa en baudios, es decir, en el número de símbolos cifrados por segundo.

Atención: según el algoritmo utilizado para transformar la información en señal, puede que el baudio tenga o no un significado de bit por segundo. Así, si se cifra un bit elemental en forma

de dos pulsos sucesivos, con el método Manchester, por ejemplo, el dispositivo tendrá que disponer de una banda de transmisión de 20 MHz (20 millones de símbolos por segundo) para una velocidad de 10 Mbps, como por ejemplo en el caso de Ethernet.

c. La utilización

	Analógicos	Digitales
Analógicos	emisoras de radio (música, voz)	CD (0 y 1 decodificados en frecuencias)
Digitales	marcación de un número de teléfono (método de impulsos) módem (señales telefónicas analógicas)	terminal y ordenador central

2. Codificación de los datos

Para la conversión de los datos en señal transportable, es necesario realizar operaciones intermedias.

La manera de cifrar los datos se llama **codificación**.

La aplicación de una codificación sobre un conjunto determinado de datos también recibe el mismo nombre, **codificación**.

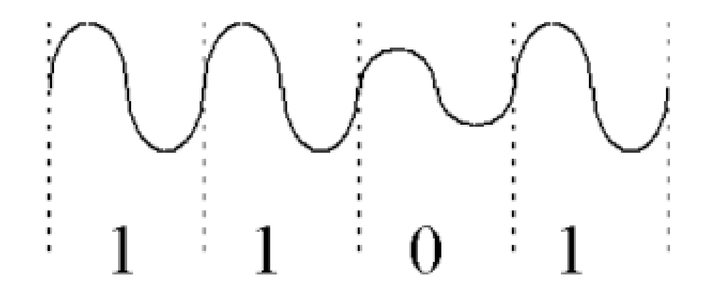
a. La codificación de los datos digitales como señales analógicas

En este caso, la señal propaga la información de forma analógica, que contiene múltiples valores. Entre ellos, solo dos, los que representan el 0 y el 1, son significativos. Se pueden utilizar diferentes modulaciones para diferenciar los datos elementales.

Amplitud modulada

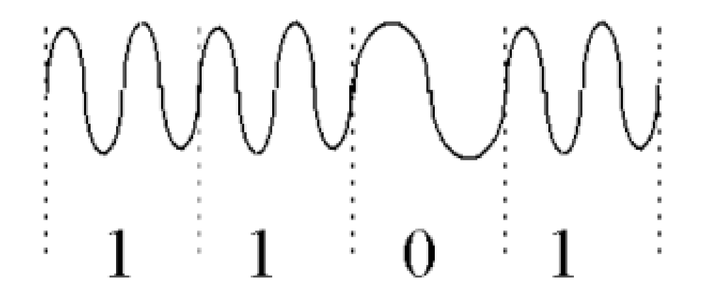
La primera y más sencilla modulación consiste en hacer variar la amplitud (AM - *Amplitude Modulation*). Este método se utiliza para las comunicaciones de larga distancia, con frecuencias bajas y de potencia muy alta, como se hace en telefonía.

En el siguiente ejemplo, la amplitud vale 1 y media amplitud, 0.



Frecuencia modulada

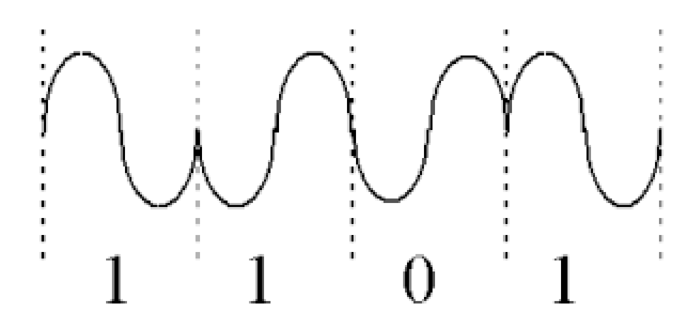
Una segunda modulación consiste en variar la frecuencia (FM - *Frequency Modulation*).



Fase modulada

La modulación de fase (PM - *Phase Modulation*) presenta básicamente dos niveles: la propia fase, cuyo grado es 0, y su fase opuesta desplazada en el tiempo, a 180°. Está especialmente recomendada para las transmisiones digitales.

En el siguiente ejemplo, el nivel 1 indica un cambio de fase; el 0, ausencia de cambio.



b. La codificación de los datos digitales en señales digitales

La codificación de los datos digitales en señales digitales se traduce a menudo en la transformación de símbolos binarios en un cierto número de señales cuadradas (o impulsos luminosos).

Existen dos maneras de efectuar estas codificaciones: bien traduciendo bit a bit los datos en señales, la llamada codificación en línea, o bien utilizando una tabla para convertir un conjunto de bits en una señal concreta, la codificación completa.

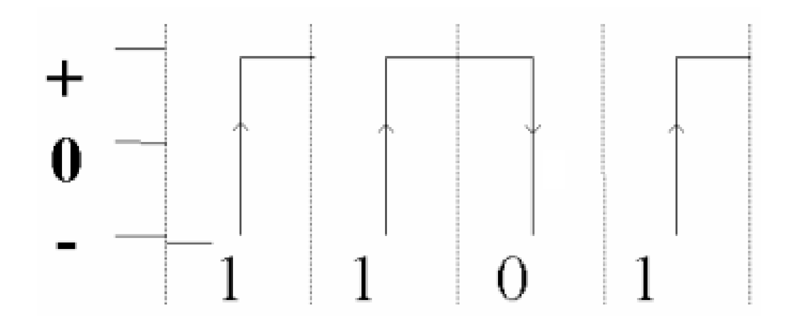
c. La codificación en línea

Hay muchos modelos de traducción de datos digitales en señales que se pueden utilizar. Aquí presentamos solo algunos ejemplos.

Manchester

'1': baja tensión, después alta tensión.

'0': alta tensión, después baja tensión.

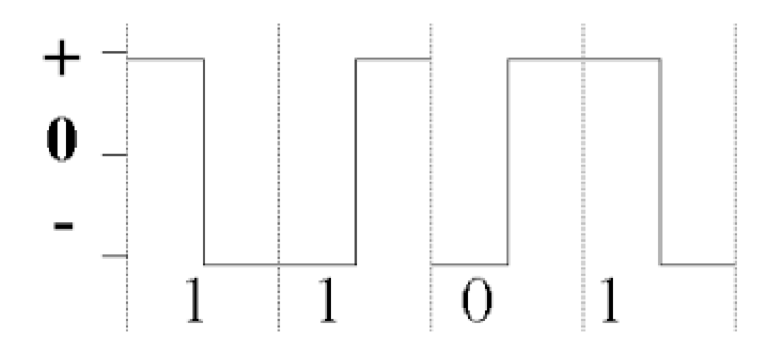


Este método se utiliza en las redes Ethernet. Las tarjetas Ethernet a 10 Mbps utilizan una frecuencia de 20 MHz. La eficacia de codificación es del 50 %, debido a que un símbolo se codifica en dos tensiones cuadradas.

Manchester diferencial

'0' se repite la señal anterior.

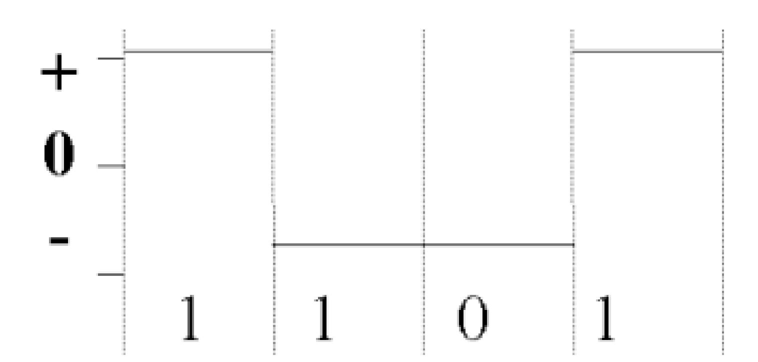
'1' se invierte la señal anterior.



Non Return to Zero, Invert on One (NRZ-1)

'0' se repite la señal anterior.

'1' se invierte la señal anterior.



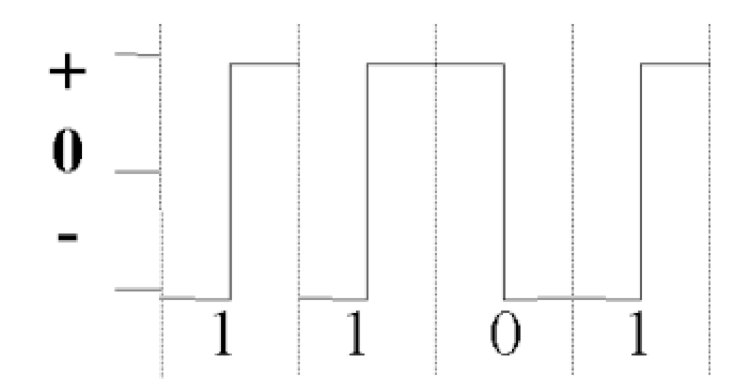
d. La codificación completa

La codificación completa requiere una mejor calidad de transmisión que la codificación en línea. Por esta razón se utilizan, sobre todo, en fibra óptica. Como ejemplo se puede citar la codificación 4B/5T (4 bits por 5 transiciones) utilizada en redes FDDI. Esta clase de codificación ofrece una eficacia del 80 % (4/5), mientras que la codificación para Ethernet es del 50 %.

3. Multiplexado de señales

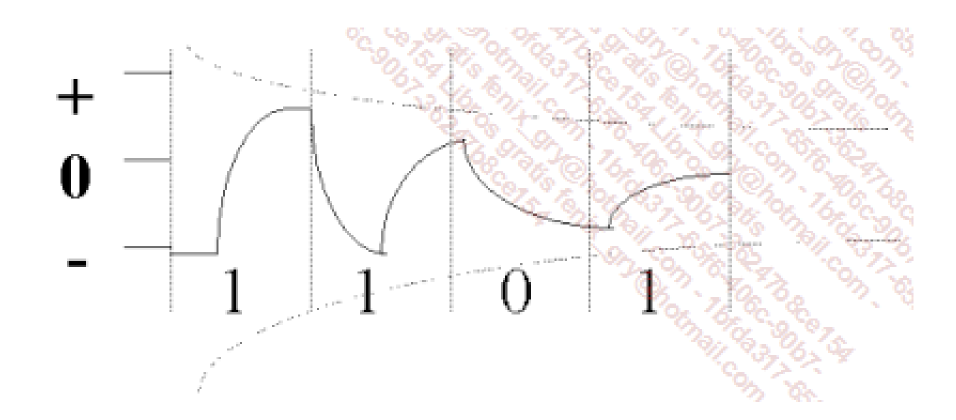
a. El sistema de banda básica

En una red de banda básica, cada dispositivo transmite de manera bidireccional. Las señales intercambiadas son digitales.



Señal original

La atenuación, la distorsión y el ruido deterioran las señales digitales muy rápidamente. Se pueden utilizar repetidores para establecer y regenerar la señal.



Señal después de la atenuación

b. El sistema de banda ancha

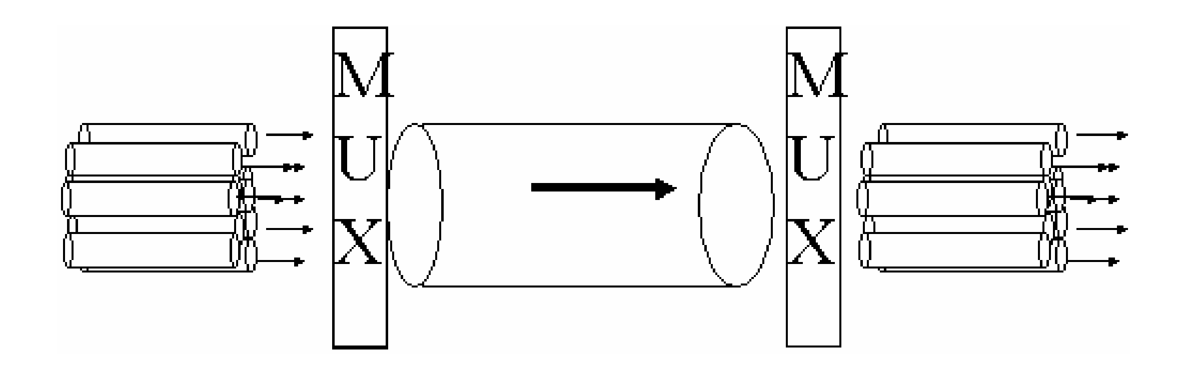
Cada dispositivo transmite de manera unidireccional. Las señales intercambiadas son analógicas.

Las señales se deterioran muy poco con respecto a la banda básica. Se utilizan amplificadores para regenerar las señales analógicas.

Es preferible hacer que los datos transiten en forma de señales analógicas en distancias importantes (p. ej. a través de módems en la RTC).

c. El multiplexado

El objetivo del multiplexado es compartir el canal de comunicación entre varios periféricos. En realidad consiste en dividir la capacidad del canal (su ancho de banda) en varios canales.



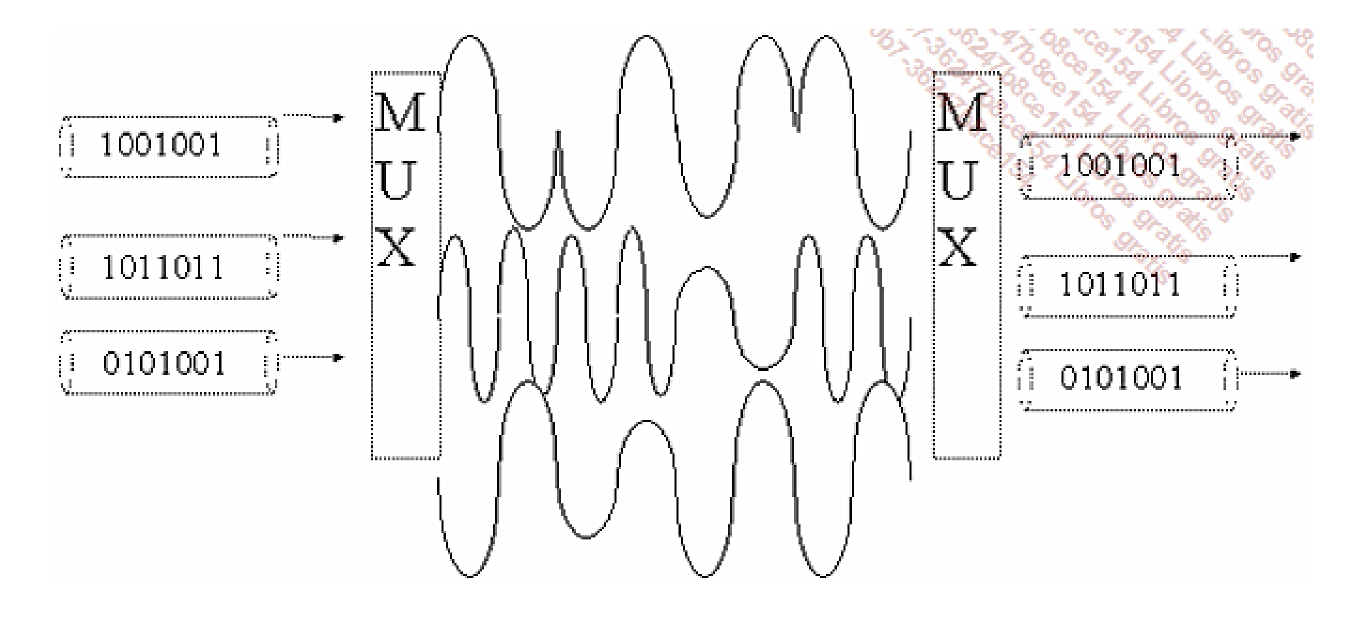
El multiplexado

Por ejemplo, se puede multiplexar un terminal y una línea X.25 de telefonía de una línea Transfix de 64 Kbps que esté comprimida.

Hablaremos de multiplexado de frecuencia cuando el canal principal transporta señales analógicas, y de multiplexado temporal cuando la señal es digital.

Multiplexado de frecuencia

Los datos de entrada se transforman siguiendo unos componentes frecuenciales muy bien elegidos (un portador de frecuencia). Así, cada portador se puede extraer a su llegada.

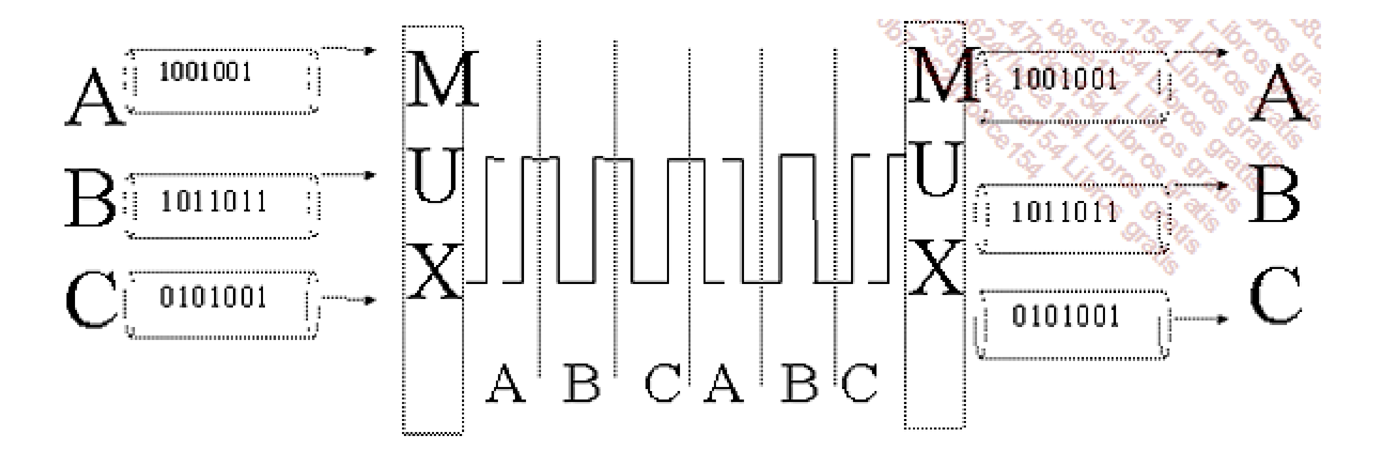


El multiplexado de frecuencia

La televisión por cable, que va a 500 MHz, es un ejemplo. Se multiplexan 80 canales en un ancho de banda de 8 MHz. A su vez, en cada uno de estos canales se multiplexan el sonido y el vídeo.

Multiplexado temporal

En el caso del multiplexado digital, los datos se transportan secuencialmente. A cada canal se le asigna una cantidad de información por cada transporte.



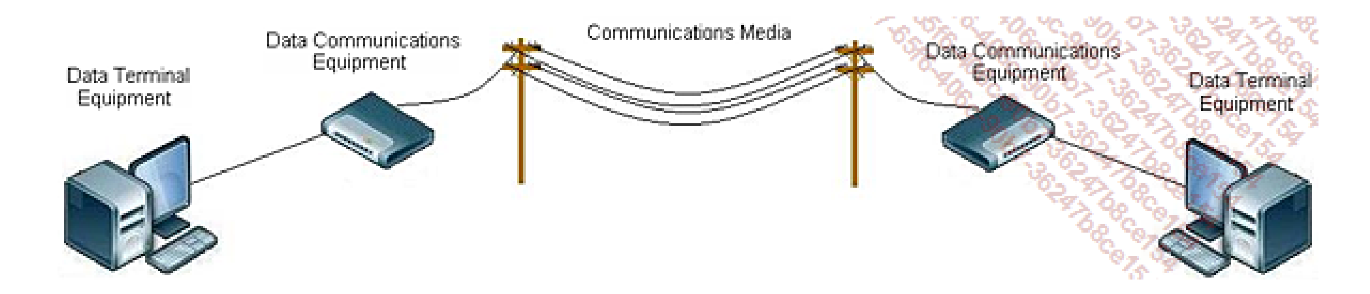
El multiplexado temporal

El inconveniente es que, si no se utiliza un canal asignado, se pierde el espacio reservado en perjuicio del resto de los canales.

Conversión de las señales

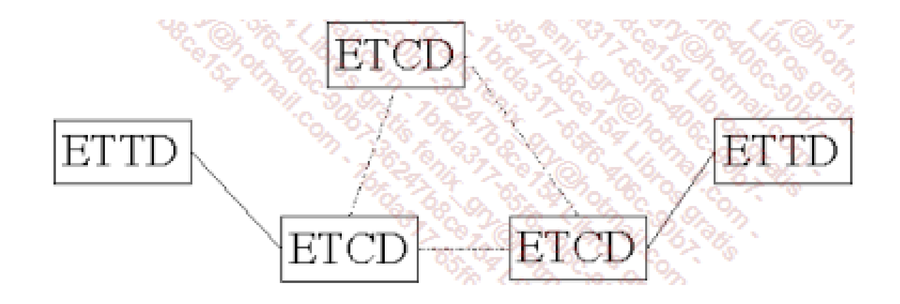
1. Definiciones

El nivel físico trabaja con las señales emitidas entre dos puntos; por un lado, en el equipo del usuario, llamado Equipo Terminal de Tratamiento de Datos (ETTD), en inglés *Data Terminal Equipment* (DTE), y en el otro lado de la red, en el Equipo Terminal de Circuito de Datos (ETCD), en inglés *Data Communications Equipment* (DCE).



Equipos terminales e intermedios

Un ETTD puede ser un ordenador o un router, mientras que un ETCD puede ser un módem, un conmutador o un multiplexor.

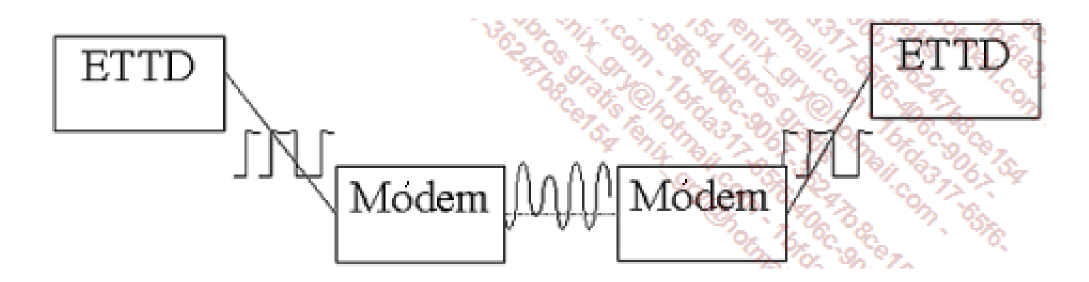


Equipos terminales e intermedios

2. Módem



La función del módem es MOdular y DEModular, es decir, codificar datos digitales convirtiéndolos en señales analógicas con el fin de hacerlas recorrer distancias considerables.



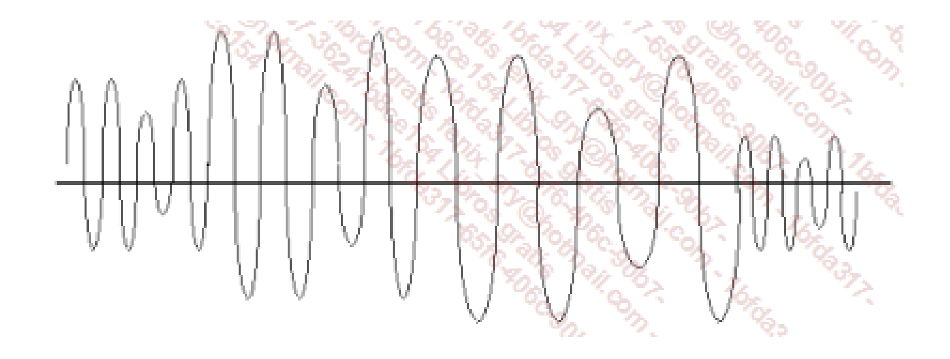
Un módem se puede utilizar para compartir un canal (en el caso de señales analógicas) a través de portadores con frecuencias diferentes.

Para distancias cortas, por ejemplo en una oficina, no es necesario un módem, ya que se pueden utilizar señales digitales (p. ej., RS232-C).

La mayoría de las veces, el módem se utiliza para establecer una conexión de punto a punto mediante la red telefónica, entre dos lugares distantes.

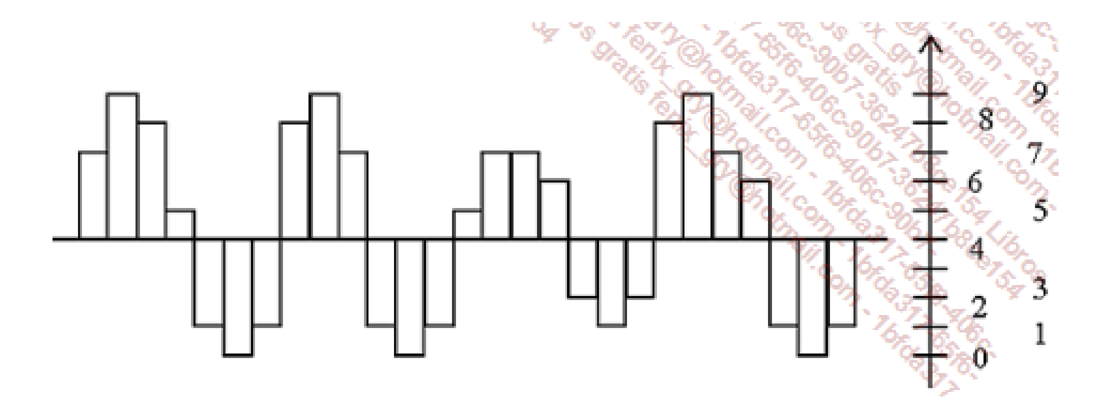
3. CODEC

La función del CODEC, COdificador DECodificacor, es la codificación de una señal analógica (que representa datos analógicos) para convertirla en una señal digital. En realidad, debe muestrear la señal, es decir, digitalizarla. Cualquier tarjeta de buena calidad integra un CODEC.



Señal original

Después de la digitalización:



Digitalización de la señal

Señal digitalizada

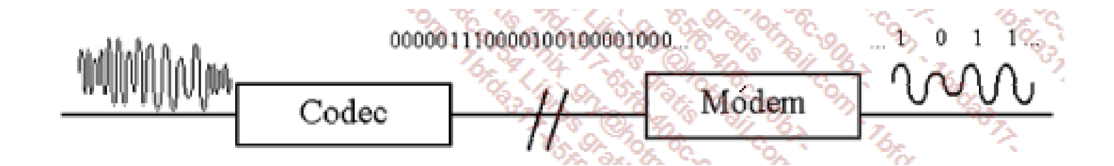
(7,9,8,5,1,0,1,8,9,7,1,0,1,5,7,7,6,2,1,2,8,9,7,6,1,0,1)

Si los datos se cifran en 8 bits (valores de 0 a 255), cada valor decimal se cifra en binario en 8 símbolos. Luego solo queda aplicar el método de codificación para cifrar los símbolos '0' y '1' en forma de señales.

Señal binaria digitalizada

(00000111,00001001,00001000, ...,0000000001,0000000000,0000000001)

Podemos imaginar que muestreamos un dato analógico en dato digital, después de transportarlo mediante una señal analógica, utilizando un módem.



Función del códec

Soportes de transmisión

Un soporte de transmisión transporta datos en forma de señales entre las interfaces de red.

Hay distintos tipos de soporte en función del precio, de la simplicidad de la instalación, la velocidad, la resistencia a las interferencias, etc.

Entre estos, se distinguen los soportes limitados y los no limitados.

1. Soportes limitados

Son soportes físicos, como los cables que conducen la electricidad.

Los principales soportes limitados son el par trenzado, el cable coaxial y la fibra óptica.

a. El par trenzado

Un par trenzado en su forma más simple está compuesto por dos cables trenzados de cobre, cada uno protegido con una cubierta aislante. Hay varios tipos de pares trenzados: el par trenzado no blindado *Unshielded Twisted Pair* (UTP) y el par blindado *Shielded Twisted Pair*(STP) son los más extendidos.

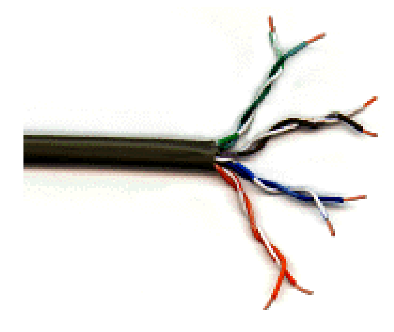
El par trenzado blindado (STP) añade una protección por par. Existe igualmente un tipo de pares FTP (*Foiled Twisted Pair*), que proporciona protección utilizando una tira de aluminio alrededor de los 4 pares. Se puede encontrar también una combinación de los dos anteriores llamada S/FTP o *Shield/Foiled Twisted Pair*. Finalmente, otro tipo de protección consistirá en una hoja doble por par y en general. Se trata de F/FTP.

El número de pares por cable varía. El trenzado de los cables disminuye las interferencias eléctricas procedentes de los pares adyacentes y del entorno exterior.

Par trenzado no blindado

Es el tipo de par trenzado más utilizado en las redes locales. Un segmento de cable UTP puede alcanzar los 100 metros.

La mayoría de los sistemas telefónicos utilizan el tipo UTP. La popularidad de este tipo de cable se debe al hecho de que en un gran número de edificios se realiza un cableado previo para los sistemas telefónicos. No obstante, el sistema telefónico debe respetar las características propias de las redes informáticas (como el trenzado) para garantizar una buena calidad de transmisión.



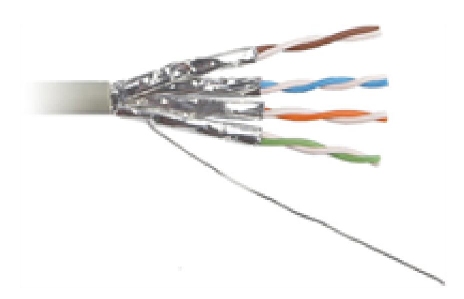
Cable de pares trenzados

Par trenzado blindado

El cable UTP es especialmente propenso a las interferencias (mezcla de señales debida a pares vecinos). El cable STP mejora la transmisión utilizando una envoltura trenzada de cobre de mejor calidad y más protectora que la empleada para el cableado UTP. Además, una envoltura de

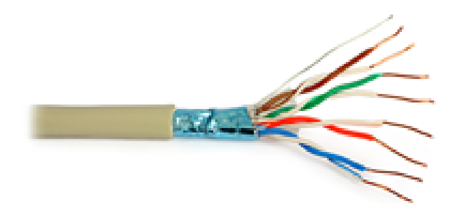
aluminio recubre cada uno de los pares trenzados.

Así, a diferencia del cable no blindado, el cable STP alcanza velocidades más elevadas para distancias ligeramente superiores.



Cable STP

El cable FTP es más resistente a interferencias externas.



Cable FTP

Conectores

Existen diferentes tipos de conectores para el par trenzado; veamos los principales a continuación:

- RJ11: cable telefónico de 2 pares trenzados.
- RJ14: cable telefónico de 3 pares trenzados.
- RJ45: cable de red de 4 pares trenzados.

Para redes de gran envergadura, es posible organizar las conexiones a partir de un armario de distribución de cables.

El conector RJ45 se utiliza hoy por todas partes, ya sea para conexiones de red o de telecomunicaciones.



Atención: no lo confunda con los conectores RJ11, utilizados en los antiguos teléfonos.



Categorías y tipos de cables de pares trenzados

El cableado UTP figura en la normativa de cableado de los edificios comerciales.

Aquí tenemos las seis categorías definidas para los cables UTP por *Electronic Industries Association and Telecommunication Industries Association* (EIA/TIA):

Categorías	Características	Tipos de datos
1 (obsoleto)	Cable telefónico UTP tradicional	Voz
2 (obsoleto)	UTP de 4 pares, puede transmitir hasta 4 Mbps	Datos
3	UTP de 4 pares con tres trenzados por pie (33 cm) que puede transmitir 10 Mbps (estándar actual)	Datos
4	UTP de 4 pares que puede transmitir hasta 16 Mbps (se utilizaba con Token Ring)	Datos
5 (1991)	UTP, STP o FTP de 4 pares, que puede transmitir hasta 100 Mbps => Ethernet 10 y 100, Token Ring 4 y 16	Datos
5e (Enhanced) 1999	UTP, STP o FTP de 4 pares, que puede transmitir hasta 1 Gbps => Ethernet 100, 1000, ATM 155	Datos
6 (2002)	La categoría 6, basada en el UTP de clase E, soporta un subconjunto de la categoría 5e => Ethernet 10G	Datos
6a	La categoría 6a (aumentada) de clase Ea soporta 1 Gbps y 10 Gbps => Ethernet 100 y 100	Datos
7	Esta categoría, basada en F/FTP de clase F, soporta hasta 10 Gbps en distancias más cortas para aplicaciones que necesiten medidas de seguridad fuertes	Datos
7a	La categoría 7 aumentada permite esperar a largo plazo velocidades de hasta 100 Gbps a unos 15 metros (40 Gbps a unos 50 metros)	Datos

El precio del cable aumenta en función de la categoría. Cada componente o conector que se utilice debe soportar la misma velocidad o las mismas limitaciones para una determinada categoría. Una vez realizada la instalación, se debe certificar la infraestructura implementada de acuerdo con la categoría utilizada.

Hoy en día, la categoría 6a comienza a extenderse: soporta tanto el 1GBase-T como el 10GBase-T.

La categoría 7 permite utilizar los 10 Gbps en condiciones de ruido elevadas.

Por último, la categoría 7a, que no utiliza conectores RJ45, no ha sido aprobada por la IEEE, que ha ratificado la 802.3ba (Ethernet 40G y 100G) en junio de 2010. No es, pues, compatible.



F/FTP categoría 7a que no utiliza los conectores RJ45

Evaluación de la calidad de los cables de pares trenzados

Las dos causas principales por las que una señal eléctrica se puede debilitar en un cable de cobre son el debilitamiento lineal (o atenuación expresado en dB/km), que caracteriza la pérdida de señal debida al tránsito a través de una gran distancia, y el debilitamiento paradiafónico constatado en pares trenzados influidos eléctricamente por los pares vecinos.

La atenuación caracteriza la pérdida de señal, que se acentúa a medida que esta recorre el cable. Cuanto más se debilita la señal (es decir, mayor es la resistencia para recorrer el cable), más atenuación tenemos.

El debilitamiento paradiafónico (NEXT - *Near End CrossTalk*) es la capacidad de un par de no ser perturbado por sus vecinos. Cuanto mayor es este parámetro, mejor es el cable.

En consecuencia, tenemos un par de buena calidad cuando la atenuación es escasa y el debilitamiento paradiafónico es elevado.

La calidad de los cables de pares trenzados pasa también por una protección contra las señales parásitas, reduciéndolas o evitando generarlas para no perturbar a los pares adyacentes.

El blindaje del par STP constituye un primer nivel de protección frente al exterior.

Otro medio consiste en transportar una tensión idéntica, pero de polaridad inversa por par, llamada método equilibrado. Estas dos señales opuestas generan una señal global que se anula para no afectar a los pares vecinos.

También hay filtros para frecuencias en Token Ring, que se llaman BALUN (*BALanced UNbalanced*).

Es necesario cuidar la protección contra motores, neones y tubos fluorescentes; para ello se utiliza un casquillo metálico que hace la función de jaula de Faraday.

b. El cable coaxial

Aunque este tipo de cable hoy en día casi no está presente en las empresas, es interesante ver cuáles son sus características para comprender la evolución de las redes informáticas.

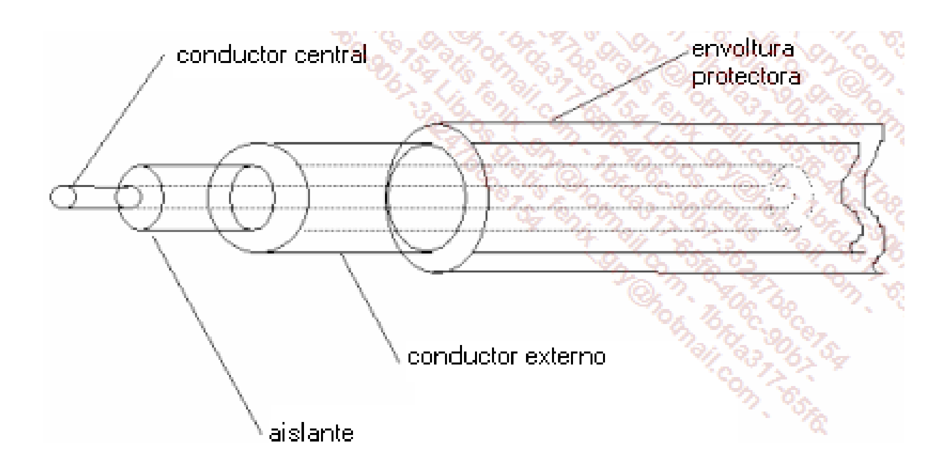
Composición

Está formado por un conductor central de cobre, por un aislante (o dieléctrico), por un segundo conductor en forma de red metálica trenzada que garantiza el blindaje y, finalmente, por una envoltura plástica que garantiza la protección mecánica del conjunto.



Cable coaxial y blindaje

Los cables coaxiales se clasifican según su impedancia característica (la impedancia es, en la corriente alterna, lo mismo que la resistencia en la corriente continua). Entonces, 50 Ohms corresponde a las transmisiones digitales y 75 Ohms a transmisiones analógicas.



RG-8, RG-11	cable coaxial grueso (12 mm de diámetro), *Ethernet grueso* o*thick Ethernet*, *50 Ohms*, *10 base 5*.
RG-58	cable coaxial fino (6 mm de diámetro), *Ethernet fino* o *thinnet*,*10 base 2*.
/U	cable central de un hilo (medianamente adaptado para redes).
A/U	cable central trenzado (utilizado en redes Ethernet de coaxial fino).
C/U	especificación militar de A/U.
RG-59	cable coaxial TV (75 Ohms).
RG-62	cable ArcNet (93 Ohms).

Cuanto más grueso sea el hilo central de cobre, más distancia podrán recorrer las señales a través del cable. El RG-58 posibilita segmentos de 185 metros como máximo, mientras que el RG-8 u 11 permite llegar a los 500 metros.

Categorías de cables coaxiales

Hay dos categorías de cables coaxiales. En la primera, la envoltura aislante se fabrica en PVC

(policloruro de vinilo). Se trata de los cables coaxiales más utilizados y menos costosos. Sin embargo, en caso de incendio, emiten humo tóxico a partir de temperaturas bajas (alrededor de 100 ºC).

La segunda categoría consta de un tipo de cables resistentes al fuego. Están fabricados con teflón, y son más caros que los anteriores. Se les califica como cable para plenum. El plenum es el espacio muerto que existe entre el falso techo y el piso de arriba y que se utiliza para realizar las conexiones en una habitación.

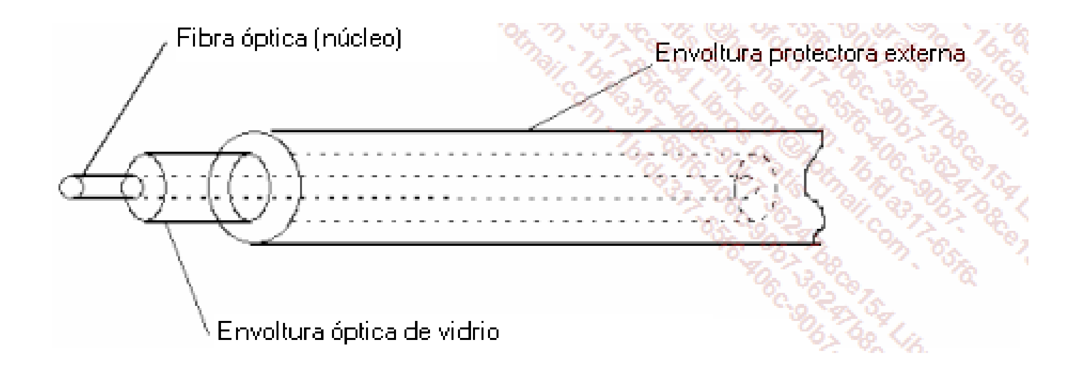
c. La fibra óptica

La fibra óptica está compuesta por una fibra conductora de luz (de vidrio o plástico) extremadamente fina (alrededor de 10 µm (micrómetros) de diámetro). La fibra transfiere datos digitales en forma de impulsos luminosos modulados. Un diodo láser emite una señal luminosa que se recupera en el otro extremo por un fotodiodo que la transforma en señal eléctrica.



Conector de fibra óptica

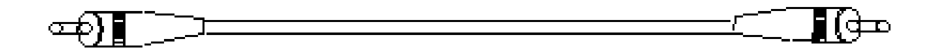
Las señales transmitidas a través de la fibra óptica están protegidas contra cualquier tipo de escucha. De hecho, y contrariamente a lo que pasa con las señales eléctricas, no es posible recoger información emitida por una onda luminosa que va a través de una fibra.



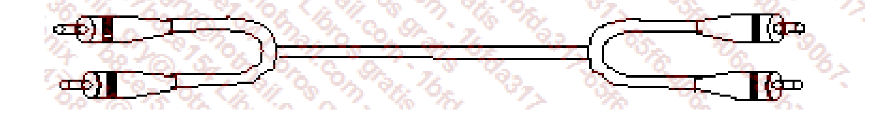
Fibra óptica

Los cables se presentan:

- en forma de una fibra única:



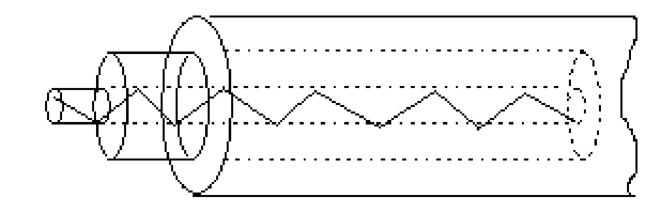
- o en forma de fibra doble con dos conectores separados:



Cable de fibra dúplex de doble fibra

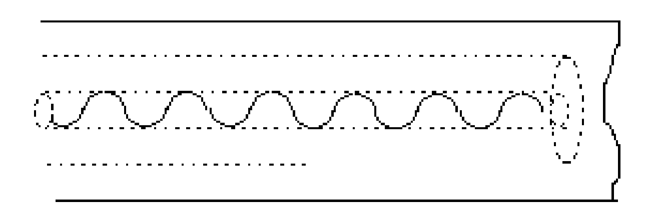
Se distinguen dos tipos de fibras: la fibra monomodo (solo transita una señal luminosa por la fibra de diámetro pequeño, cuyo núcleo es de 2 a 8 µm) y la fibra multimodo (varias señales luminosas

transitan por la fibra de diámetro más extenso, de 50 a 125 µm).



Fibra de índice escalonado

El impulso luminoso se refleja en la envoltura óptica de vidrio. Entre la categoría de las fibras multimodo, se distinguen las de índice gradual (onda sinusoidal) de las de índice escalonado (refracción en ángulo recto). En una fibra de índice gradual, el índice de refracción decrece desde el centro hacia la periferia. En una fibra de índice escalonado, no hay degradación del índice de refracción.



Fibra de índice gradual

La fibra es muy utilizada para interconectar redes locales Ethernet. De hecho, con la 10BaseFL, y la Ethernet 10 Mbps sobre fibra, es posible utilizar repetidores mixtos (fibra/coaxial o fibra/par trenzado).

La fibra solo permite la transmisión de señales en un único sentido. Por ello, a menudo nos encontraremos con las versiones de dos núcleos o de doble fibra (dos cables unidos) para la emisión y la recepción.

La fibra es ideal para la transmisión a alta velocidad de grandes volúmenes de datos (en general 10 Gbps que pueden llegar a 10 Tbps), debido a la pureza de las señales, a la ausencia de atenuación y a la insensibilidad a las interferencias eléctricas. Permite la transmisión de datos a distancias que pueden alcanzar varios miles de kilómetros.

d. Los criterios de elección de los diferentes medios

Se pueden seleccionar distintos criterios para elegir los posibles medios de transmisión.

Generalmente se considera el coste, el tipo de soporte para la banda de transmisión, la atenuación de la señal, la resistencia a los fenómenos electromagnéticos circundantes o también la simplicidad o complejidad de la instalación. En función del entorno y del tipo de la señal transportada, aparecen una serie de dificultades. Por ejemplo, podemos citar la longitud máxima de un segmento o el número de dispositivos conectados.

En el siguiente cuadro, exponemos un resumen de los principales soportes utilizados.

Características	Par trenzado no blindado (UTP)	Par trenzado blindado (FTP)	Fibra óptica
Precio del cable	Económico (los edificios además suelen estar	Más caro que UTP	El soporte más caro de todos, aunque los precios

	cableados)		están bajando
Longitud de un segmento	100 m	Un poco mayor que UTP	2000 m
Velocidad habitual	100 Mbps (cat 5) 1 Gbps (cat 5e y 6) 10 Gbps (6a y 7)	100 Mbps (cat 5) 1 Gbps (cat 5e y 6) 10 Gbps (6a y 7) Adaptados a entornos con interferencias	De 100 Mbps a 1 Gbps
Instalación	Muy sencilla	Muy sencilla	Las conexiones de fibra deben implementarse de manera que no se bloquee el paso de la luz. Además debe respetarse un radio mínimo de curvatura
Atenuación	Elevada	Escasa	Ninguna
Sensibilidad a las interferencias	Sensible	Poco sensible	Ninguna
Utilización habitual	Redes de oficina o de tamaño mediano	Entornos con interferencias o de gran tamaño	Necesidad de alta velocidad, interconexión entre distribuidores o edificios

2. Soportes no limitados

La tecnología de red inalámbrica aún no está lista para sustituir a los soportes limitados, debido, sobre todo, al pequeño ancho de banda, pero aun así es un buen complemento.

Estas tecnologías se encuentran en todos los ámbitos de la red. A veces la letra «W», de Wireless, colocada junto al acrónimo del ámbito, especifica que la red utiliza la interfaz inalámbrica. Para indicar que la red inalámbrica utiliza las ondas radioeléctricas, se utiliza la letra «R», de Radio.

Estas tecnologías permiten la movilidad de los usuarios en el interior de las oficinas o lugares de trabajo (itinerancia) o en el exterior (nomadismo).

a. Los infrarrojos

En este caso, se utiliza un haz de luz infrarroja para transmitir datos. Estas señales son muy sensibles a las luces potentes. No obstante, es posible alcanzar velocidades de unos 16 Mbps en distancias teóricas de algunos kilómetros.

Hay redes llamadas de visibilidad directa o por difusión (la señal rebota en las paredes de color claro, las paredes oscuras absorben las señales).

Lo interesante de esta tecnología es que los equipos no son muy costosos, ya que se fabrican en grandes cantidades. Es una solución que se adapta muy bien en interiores, pero que en exteriores no es utilizable debido a su sensibilidad a las condiciones atmosféricas.

En el capítulo Capas bajas de las redes personales y locales, veremos la solución irDA con más detalle.

b. El láser

Como en el caso de la transmisión por infrarrojos en visibilidad directa, esta técnica requiere un campo de visibilidad directa, ya que es sensible al problema de la alineación (entre el láser y el fotodiodo). Sin embargo es resistente a las interferencias y perturbaciones, aunque sensible a las condiciones atmosféricas.

c. Las ondas de radio terrestres

La tecnología de transmisión por ondas de radio es la mejor valorada actualmente, cualquiera que sea el tamaño de la red. En lugar de las ondas de banda estrecha, se suele preferir las ondas de amplio espectro (*spread spectrum*), más resistentes a las interferencias.

Los usos de estas redes son múltiples. Por ejemplo, a través de puentes inalámbricos se pueden interconectar redes locales sin utilizar soportes limitados.

La llegada de ordenadores portátiles y otros periféricos móviles democratizó, a través de Bluetooth o Wi-Fi, el uso de las redes de radio para los usuarios.

Las nuevas generaciones de telefonía móvil también permiten la transmisión de datos.

d. Las ondas de radio por satélite

Los sistemas de microondas permiten interconectar edificios distribuidos por zonas relativamente poco amplias. Es el método más utilizado en Estados Unidos para transmitir a través de largas distancias. Se obtienen resultados excelentes a través de dos puntos cuya visibilidad es directa (un satélite en órbita geoestacionaria y una conexión terrestre, entre dos edificios o a través de grandes extensiones).

En este último caso es necesario disponer de una homologación, de dos transmisores-receptores de radio, así como de antenas direccionales que deben ubicarse adecuadamente.

En el caso de estaciones de microondas vía satélite, es posible utilizar estaciones terrestres móviles (avión, barco).

Configuración de la tarjeta de red

La puesta en marcha de una tarjeta de red implica una parametrización a nivel de hardware del periférico, que hoy asume la funcionalidad Plug and Play, y la instalación del controlador (*driver*) de la tarjeta.

1. Configuración del hardware

En anteriores generaciones de tarjetas era necesario configurar manualmente los parámetros con ayuda de interruptores o con puentes. Posteriormente estos ajustes se hicieron con software.

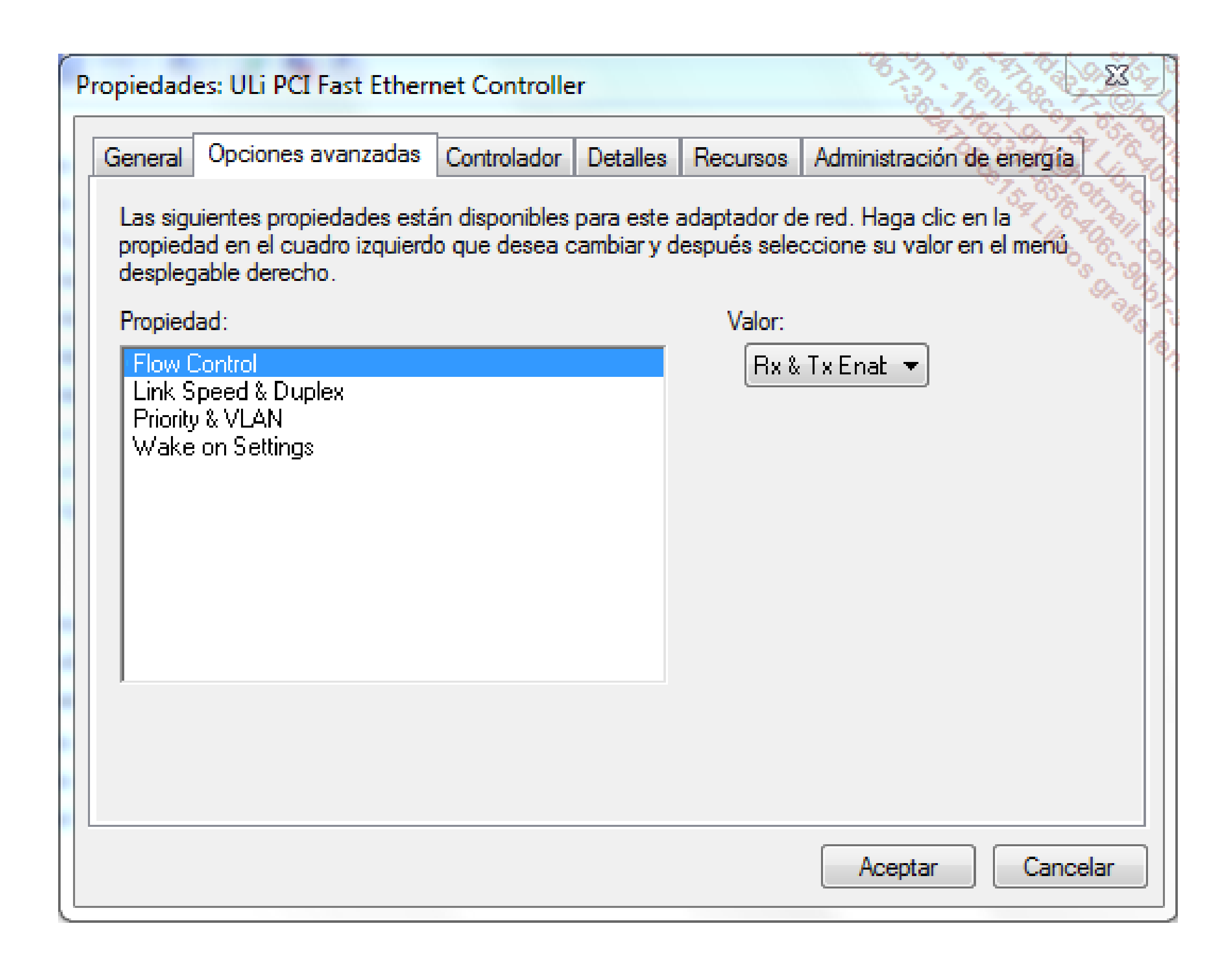
Ahora, las tarjetas son Plug and Play y autoconfigurables. Los parámetros como la línea de petición de interrupción (IRQ - *Interruption ReQuest*) y el intervalo de memoria se configuran automáticamente.

Si la interfaz de red no está integrada en la placa base, basta con apagar el ordenador e instalarla en el conector adecuado.

2. Configuración de software

Al encender el ordenador se detecta la interfaz y se efectúa la elección de los valores que deben utilizarse, sin que entre en conflicto con otros periféricos. La modificación manual de los recursos de la tarjeta de red es una tarea para especialistas que cada vez se lleva a cabo con menor frecuencia.

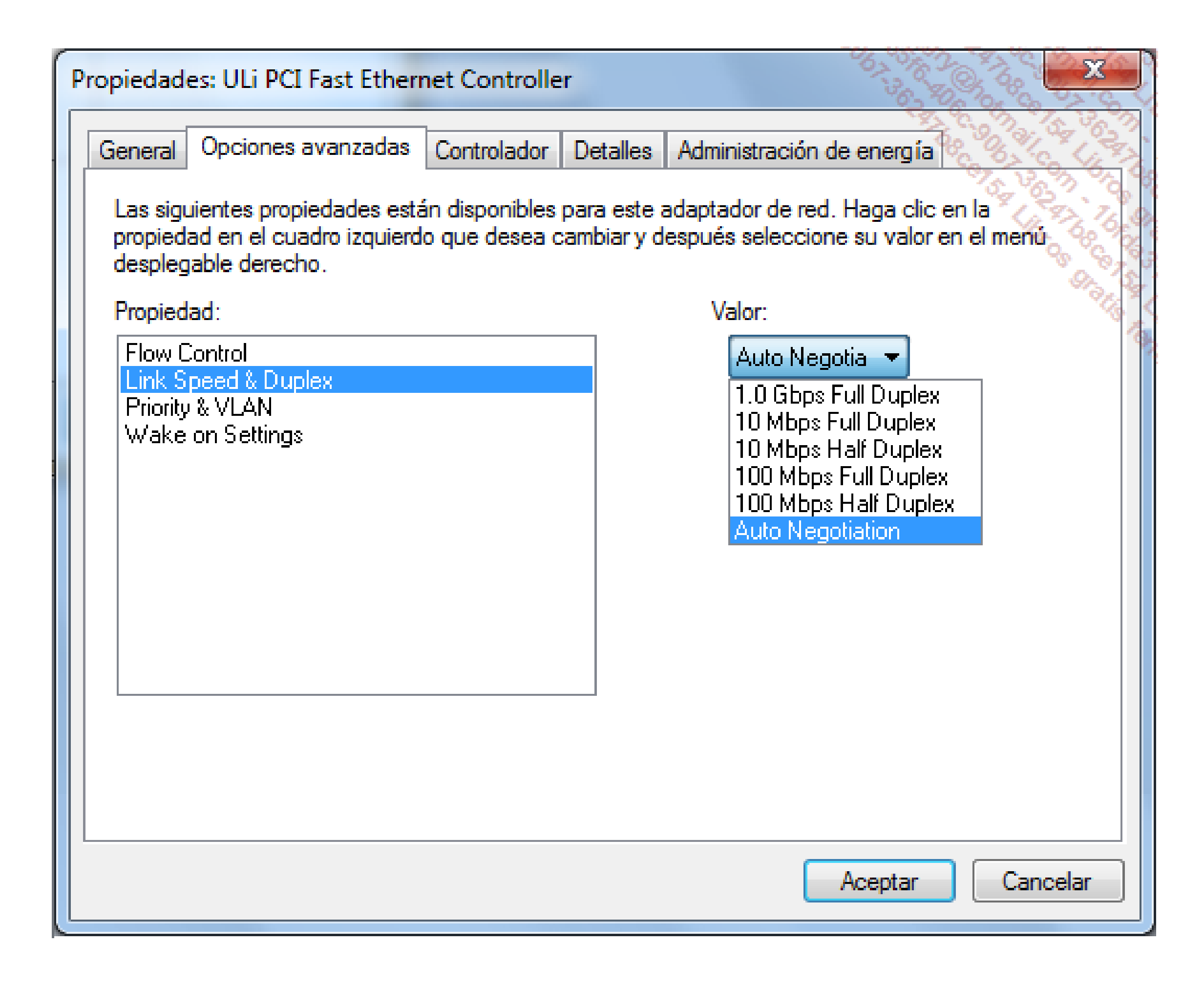
La mayor parte de las tarjetas de red no permiten el acceso a esta información.



Propiedades de la tarjeta de red en Windows 7

El propio sistema operativo elige la velocidad en función de la capacidad de la tarjeta y de la

velocidad máxima autorizada en la red a la cual se conecta. El modo de funcionamiento también se fija en función de las posibilidades detectadas. El modo integral (*full-duplex*) permite recibir y emitir simultáneamente. Si este no está disponible, se opera en modo semi (*half-duplex*). La dirección física, o *Medium Access Control* (MAC), provista por la tarjeta es la que se utiliza por defecto.



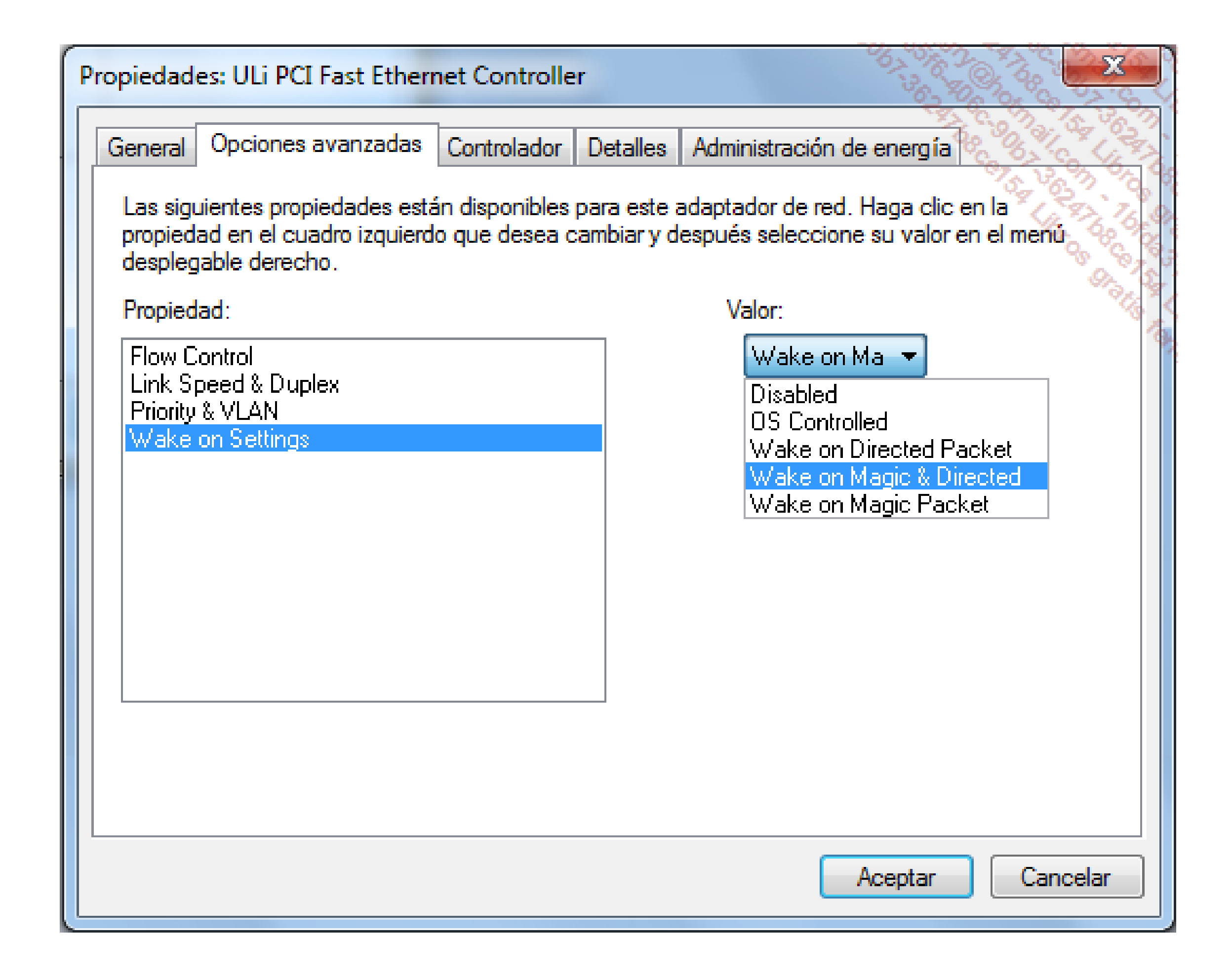
Configuración de la velocidad de una tarjeta 10/100/1000 Mbps en Windows 7

Estos valores se pueden modificar, pero se deben conocer muy bien estos parámetros para evitar un mal funcionamiento del dispositivo.

Lo único que falta para terminar la instalación del dispositivo es instalar el controlador adecuado para la tarjeta de red.

El concepto **Green IT** es cada vez más importante hoy en día. Las empresas han tomado conciencia de los retos económicos que conlleva, sobre todo en lo que se refiere a la reducción del consumo eléctrico que puede conseguirse. Por esto, uno de los puntos de entrada es **Wake On LAN** o el arranque del ordenador a distancia desde la tarjeta de red.

Las opciones para administrar este tema están disponibles directamente a nivel de la tarjeta de red:



Configuración Wake On LAN de una tarjeta de red

Imagine la cantidad de energía eléctrica que se podría ahorrar si una empresa forzara el apagado de los puestos de trabajo por la tarde, teniendo la posibilidad de arrancarlos automáticamente por la noche para desplegar parches o actualizaciones. Una vez se ha efectuado la actualización, el equipo se apagaría a distancia automáticamente.

3. Especificaciones NDIS y ODI

Las especificaciones de controlador de red *Network Device Interface Specification* (NDIS) y *Open Data Interface* (ODI) facilitan la independencia entre la tarjeta de red y los protocolos de capas superiores.

Así, la tarjeta de red se puede asociar a través de software a protocolos TCP/IP o a cualquier otro protocolo. Además, una misma tarjeta puede utilizar varios protocolos.

El tipo de especificación depende del sistema operativo utilizado. El ODI fue desarrollado por Novell y Apple, NDIS por Microsoft y 3Com.

Los sistemas operativos Windows, por ejemplo, utilizan NDIS, que define una interfaz de comunicación con la capa de Conexión de datos. Los niveles de especificación NDIS son:

- NDIS 2.0: define los controladores en modo real (MS-DOS, Windows for Workgroups 3.1 u OS/2).
- NDIS 3.0, que describe un tipo de funcionamiento de los componentes en modo extendido, es decir, que el periférico puede ser administrado a través de un contexto no exclusivo, contrariamente al modo real (p. ej., Windows for Workgroups 3.11).
- NDIS 3.1, que hace referencia a Windows 95.
- NDIS 4.0, que introduce Plug and Play (Windows 95 OSR2, NT 4.0, Windows CE 3.0).
- NDIS 5.0, que mejora estos principios y que se utiliza desde Windows 98, 98 SE, ME y 2000.

- NDIS 5.1: hace referencia a los sistemas operativos Windows XP, Server 2003 y Windows CE 4.x, 5.0.
- NDIS 5.2, a partir de Windows Server 2003 SP2.
- NDIS 6.0, que optimiza los rendimientos del controlador y mejora la seguridad, soportando igualmente Wi-Fi en modo nativo (Windows Vista).
- NDIS 6.1, relativo a los sistemas operativos Windows Vista SP1 y Windows Server 2008 (SP1 implícito).
- NDIS 6.2: hace referencia a Windows 7 y Windows Server 2008 R2.

Instalación y configuración del controlador de la tarjeta de red

1. Principios

La instalación del software de una tarjeta de red comienza por la instalación de su controlador (*driver*). Es posible que podamos utilizar el proporcionado por el sistema operativo o necesitar la utilización de los proporcionados por el fabricante (en CD o a través de Internet).

La descarga de un controlador desde el sitio del fabricante permite obtener la última versión desarrollada. En contraposición, puede que este controlador no sea estable.

A veces, se pueden obtener herramientas complementarias de configuraciones específicas, que complementan las funciones del sistema operativo, destinadas a las comunicaciones por cable (por ejemplo, Ethernet) o a las inalámbricas (por ejemplo, Wi-Fi).

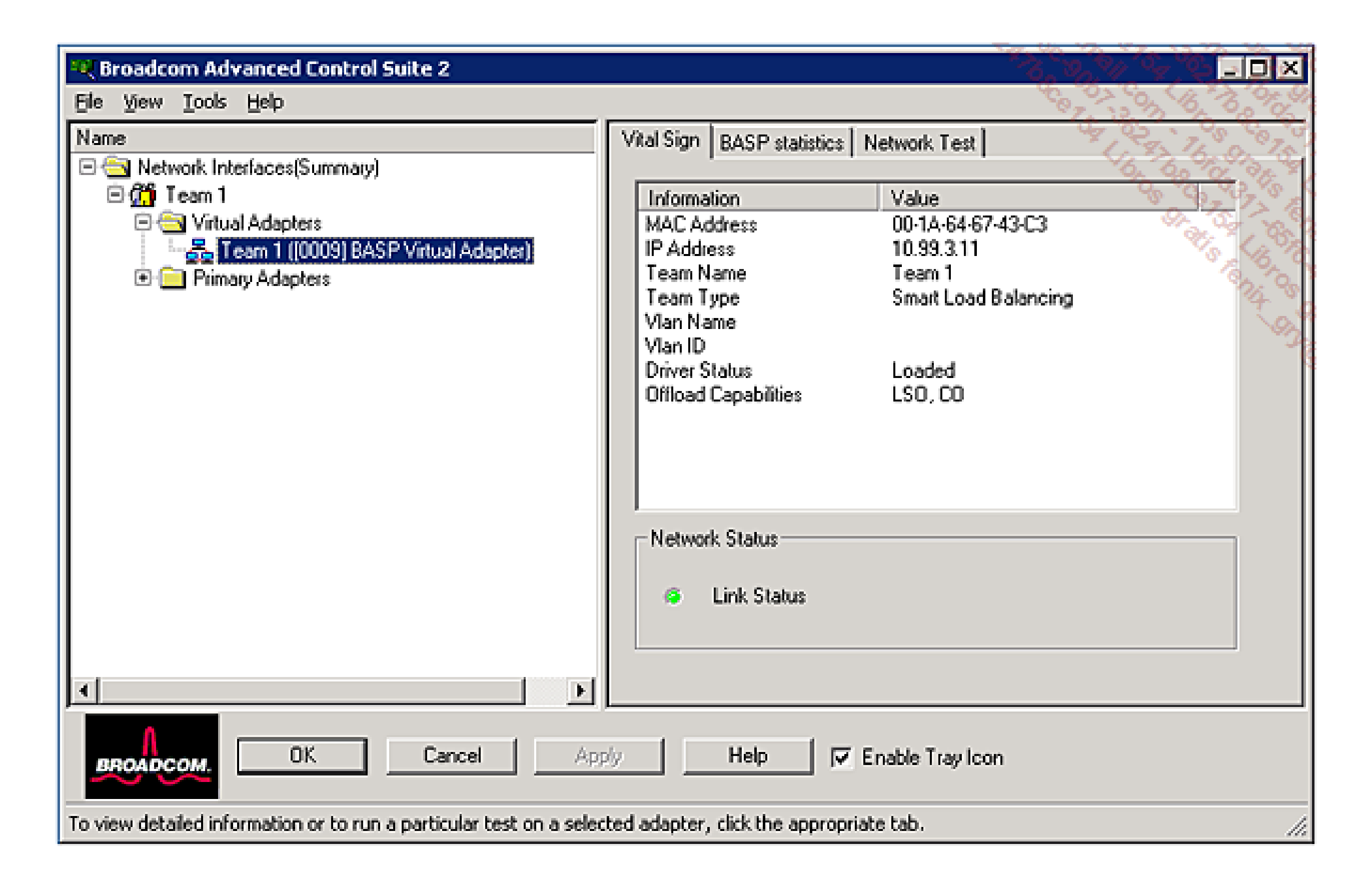
Según el sistema operativo, los procedimientos de instalación son más o menos complejos. Por ejemplo, cuando se trata de integrar un nuevo controlador de tarjetas de red aún no desarrollado para sistemas operativos Linux. Este planteamiento específico se describe un poco más adelante en este mismo capítulo.

2. Utilización de una herramienta proporcionada por el fabricante

Igual que para los controladores, puede ser interesante buscar herramientas en los sitios Web de los fabricantes de tarjetas, donde están más actualizados.

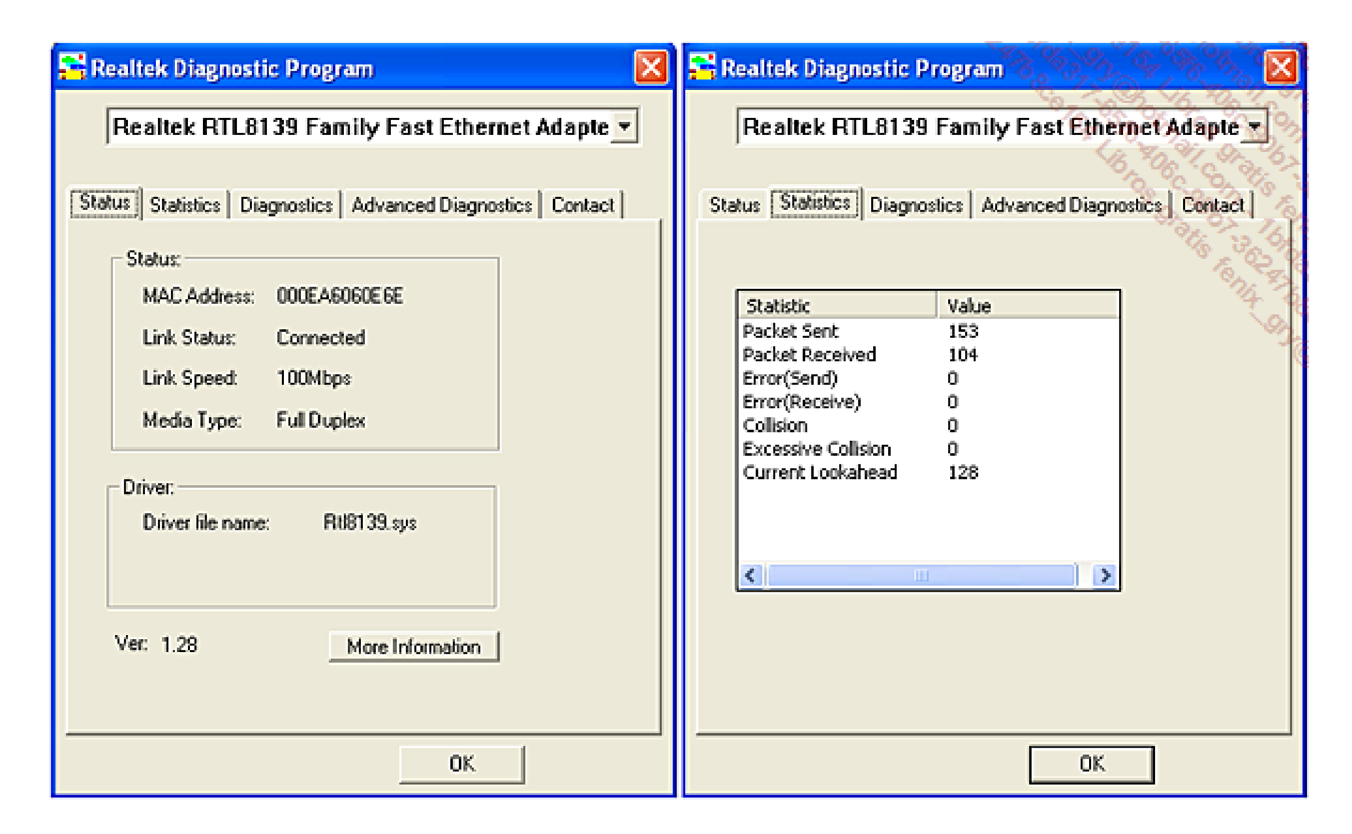
El primer grupo de herramientas que se ofrece permite remplazar los proporcionados por el sistema operativo. Sirven esencialmente para configurar la interfaz de red con mayor precisión, ya que son específicas para cada fabricante, es decir, a la carta, y no genéricas.

Como vimos en el capítulo Transmisión de datos en la capa física, las herramientas destinadas a los servidores pueden incluir funciones de puesta en marcha de «Teaming». Permiten agrupar tarjetas de red en una sola interfaz virtual, aportando un elemento de tolerancia a fallos.



Interfaz virtual por «Teaming» con la herramienta de Broadcom

También se pueden obtener herramientas de diagnóstico y de pruebas, incluso directamente desde la interfaz de configuración.



Ejemplo de herramienta de fabricante

3. Utilización del sistema operativo

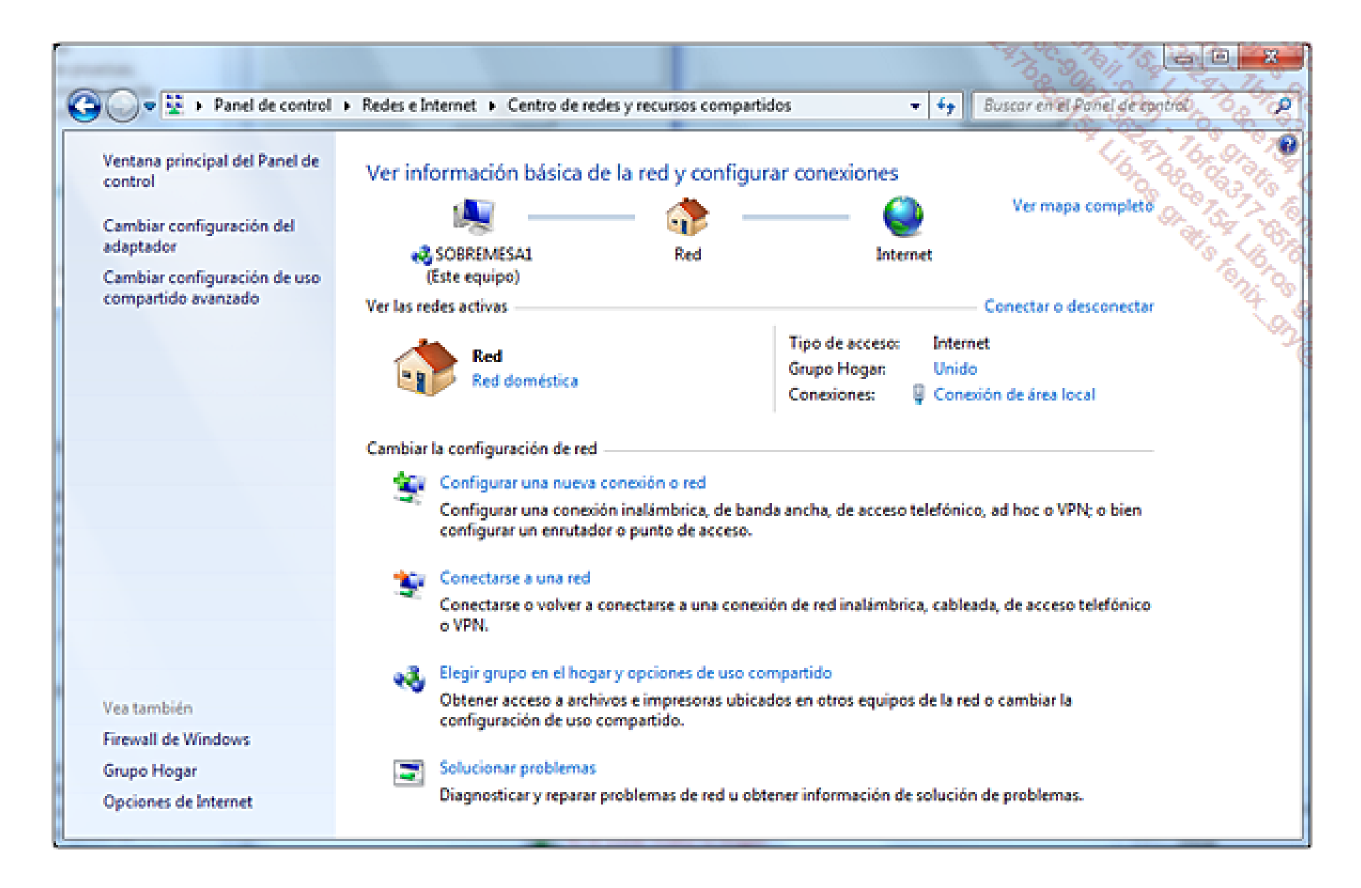
Vamos a examinar los procedimientos de instalación de una tarjeta de red en MS Windows, Linux

Red Hat, Mac OS X y Android.

a. En Windows 7 o 2008 R2

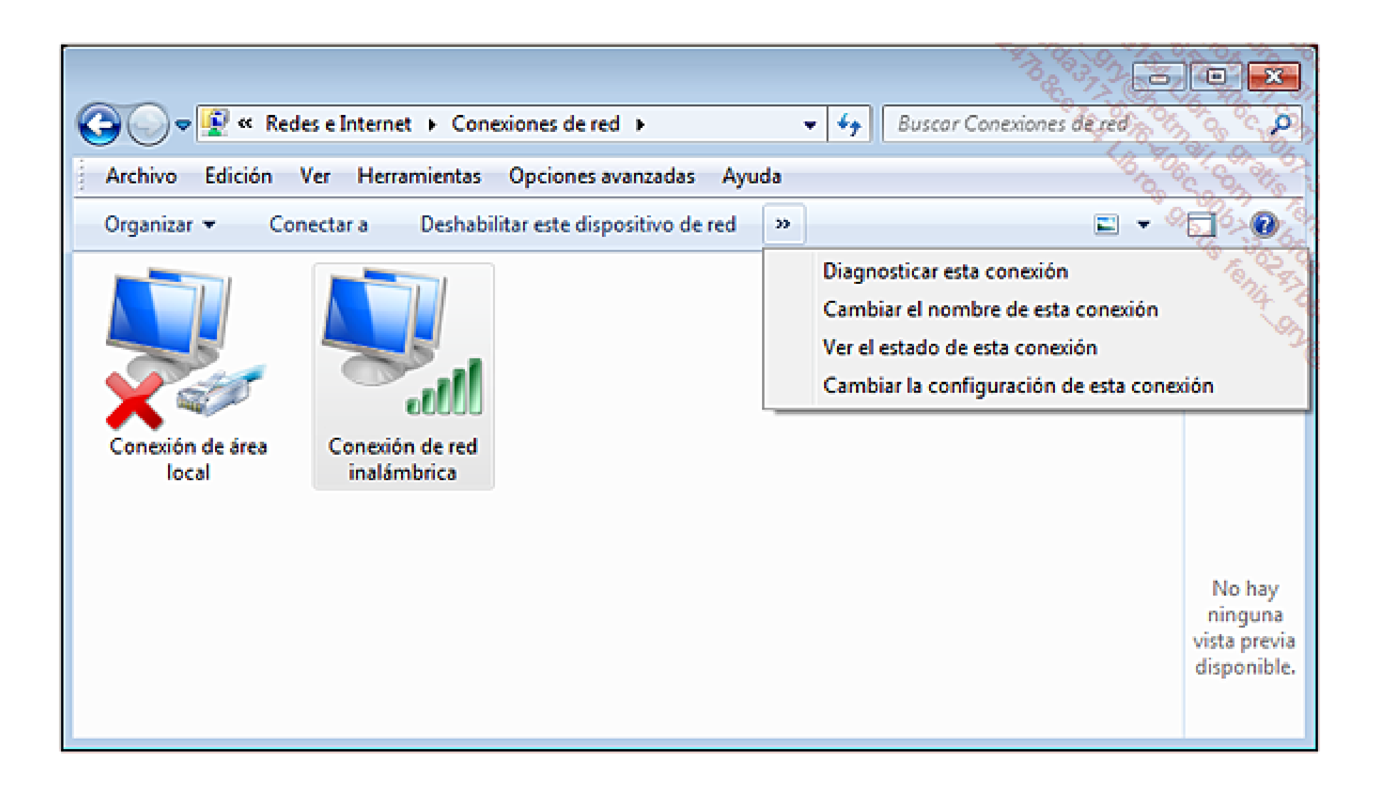
En Windows 7, los equipos de trabajo destinados a profesionales y particulares tienen la misma base. Como para Windows 2008 R2 (para servidores), el núcleo es la versión 6.1. Aunque las interfaces gráficas de los sistemas destinados a los equipos de trabajo o servidores no sean idénticas, la configuración de las tarjetas de red son similares. Además, los controladores de periféricos son comunes.

Desde el menú **Iniciar**, basta con buscar **Centro de redes y recursos compartidos** para acceder al entorno de configuración de redes de Windows 7:



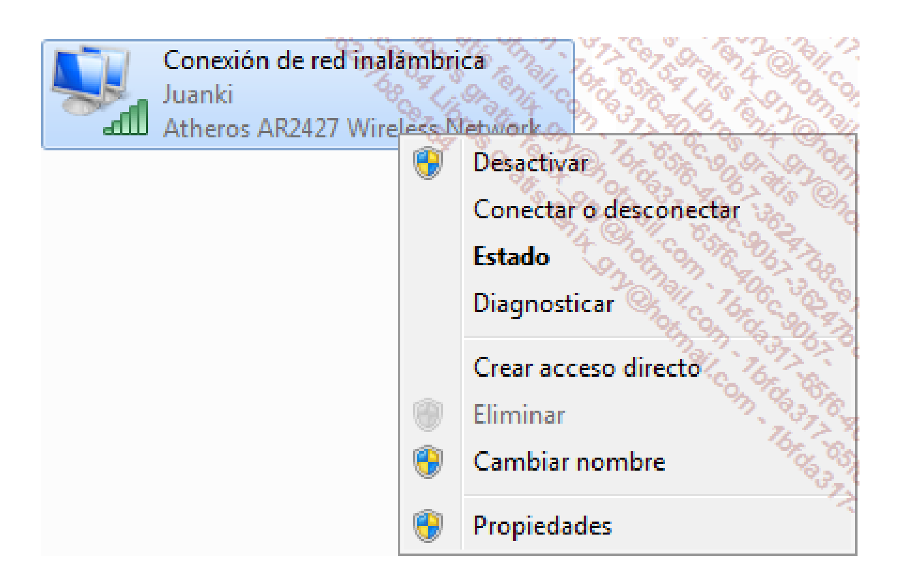
Centro de redes y recursos compartidos de Windows

El link **Cambiar configuración del adaptador** permite acceder a la configuración de las tarjetas de red del ordenador:



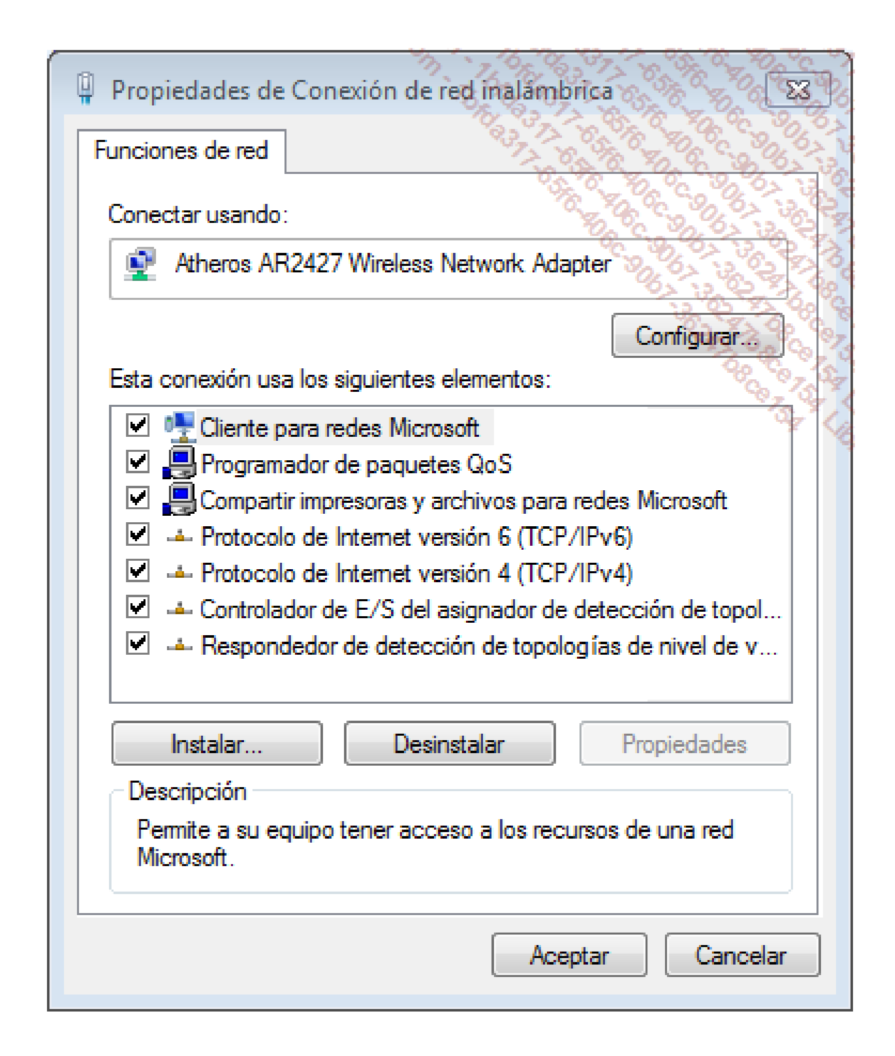
Menú contextual asociado a una conexión de red inalámbrica

En función del contexto, hay numerosas opciones; por ejemplo, para **Conexión de red inalámbrica**:



Acceso a las propiedades de la conexión inalámbrica

Ahora es posible acceder a las diferentes propiedades, sean de software o de hardware:



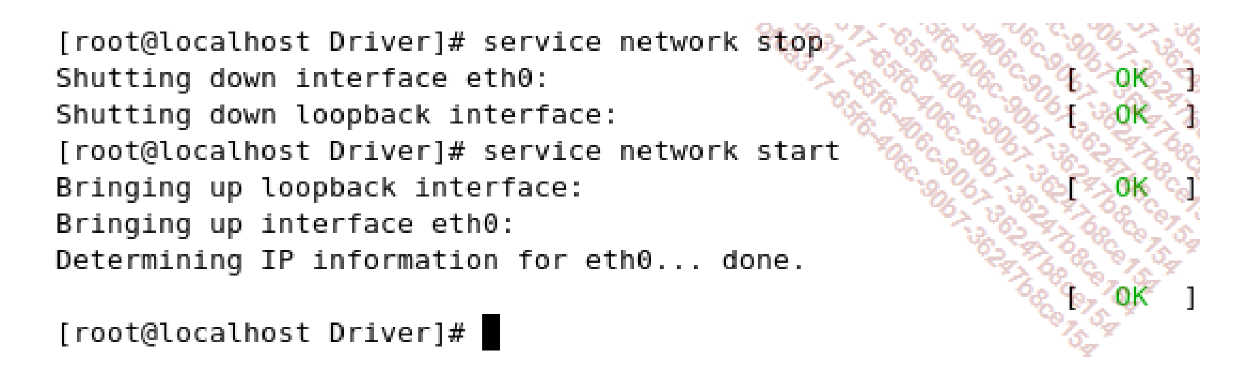
Configuración de red

b. En Linux Red Hat

Los diferentes sistemas operativos desarrollados en el núcleo de Linux han evolucionado mucho. La instalación de componentes cotidianos, entre otros, no es más complicada que en Windows.

Hemos escogido para nuestro ejemplo Linux Red Hat, que se ha especializado hasta convertirse en sistema operativo de empresa. Lo que vamos a ver refleja lo que encontramos en el resto de las versiones de un sistema operativo de este tipo.

Por ejemplo, si se detecta la tarjeta de red Ethernet durante la instalación del sistema, se asocia a su controlador y a una interfaz llamada **eth0** (denominación de Unix). Esta denominación se puede cambiar. Los servicios de red que estén asociados a ella arrancan automáticamente con el sistema.


```
[root@localhost Driver]# service network stop
Shutting down interface eth0:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
[root@localhost Driver]# service network start
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:
Determining IP information for eth0... done.
                                                           [  OK  ]
[root@localhost Driver]#
```

Arranque de los servicios de red de Linux

Durante la etapa gráfica de la instalación del sistema, si la tarjeta de red se ha detectado correctamente, un cuadro de diálogo permite parametrizar TCP/IP, como se puede ver en la

siguiente pantalla.

RED HAT
ENTERPRISE LINUX 5

Network Devices

Active on Boot	Device	IPv4/Netmask	IPv6/Prefix
☑	eth0	DHCP	DHCP

Edit

Hostname

Set the hostname:

automatically via DHCP

manually localhost.localdomain (e.g., host.domain.com)

Miscellaneous Settings

Gateway:

Primary DNS:

Secondary DNS:

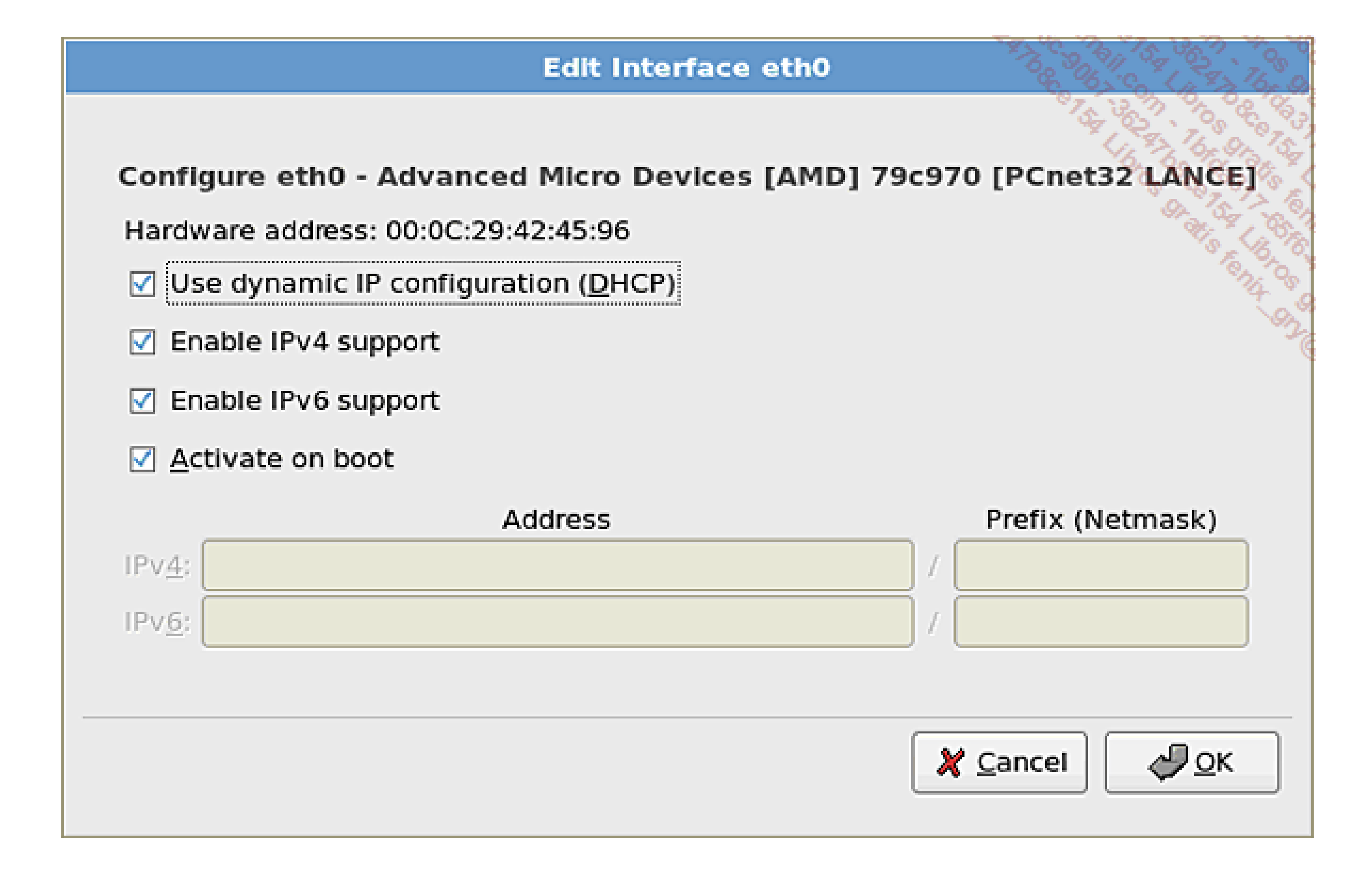
Release Notes

Back

Next

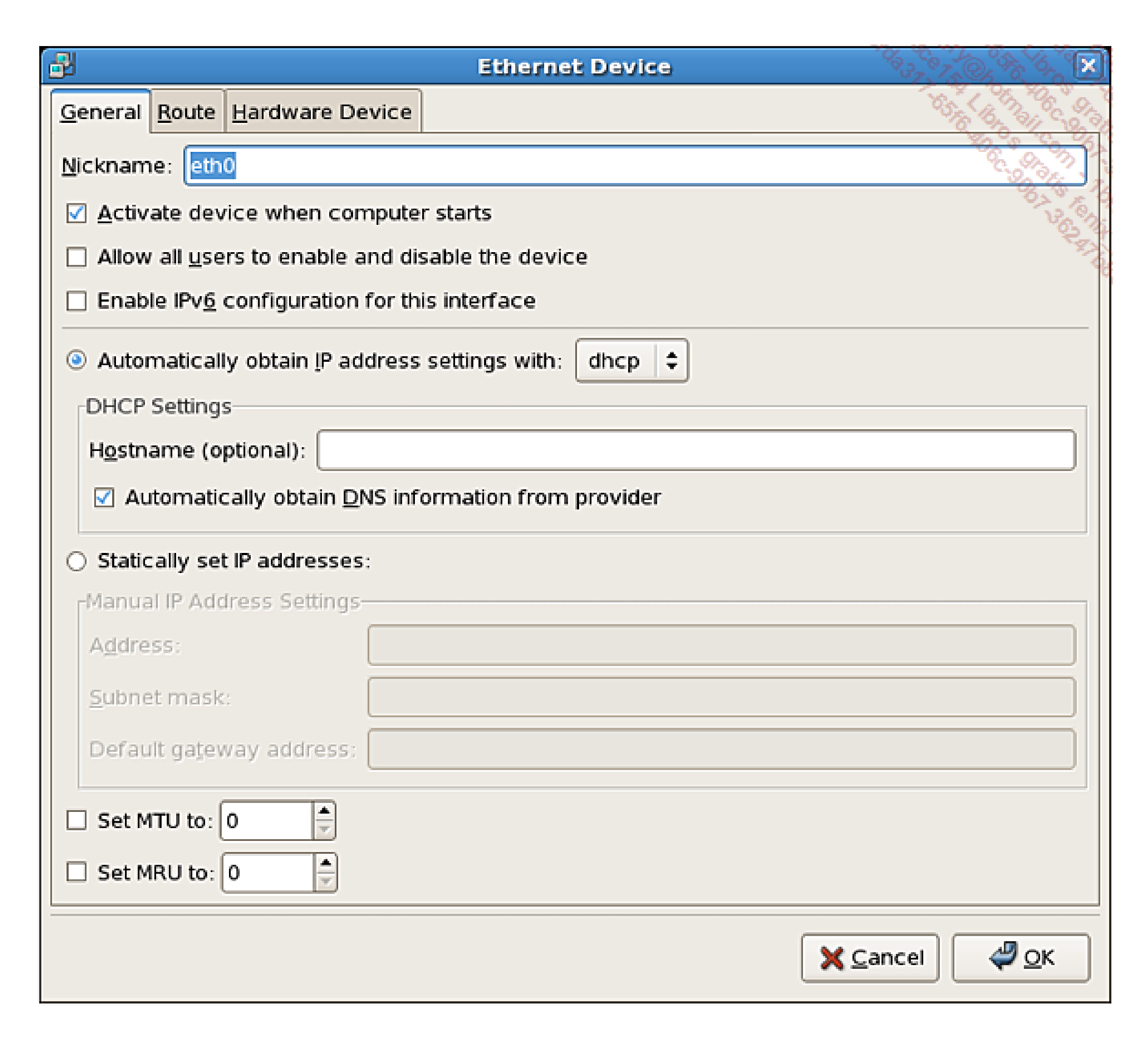
Configuración de capa media, la tarjeta se ha detectado correctamente durante la instalación

La configuración avanzada es fácilmente comprensible si se domina TCP/IP. Volveremos a este concepto más adelante. Observamos que, igual que para Windows, la configuración básica de la tarjeta, la que se refiere al hardware, es mucho más transparente.



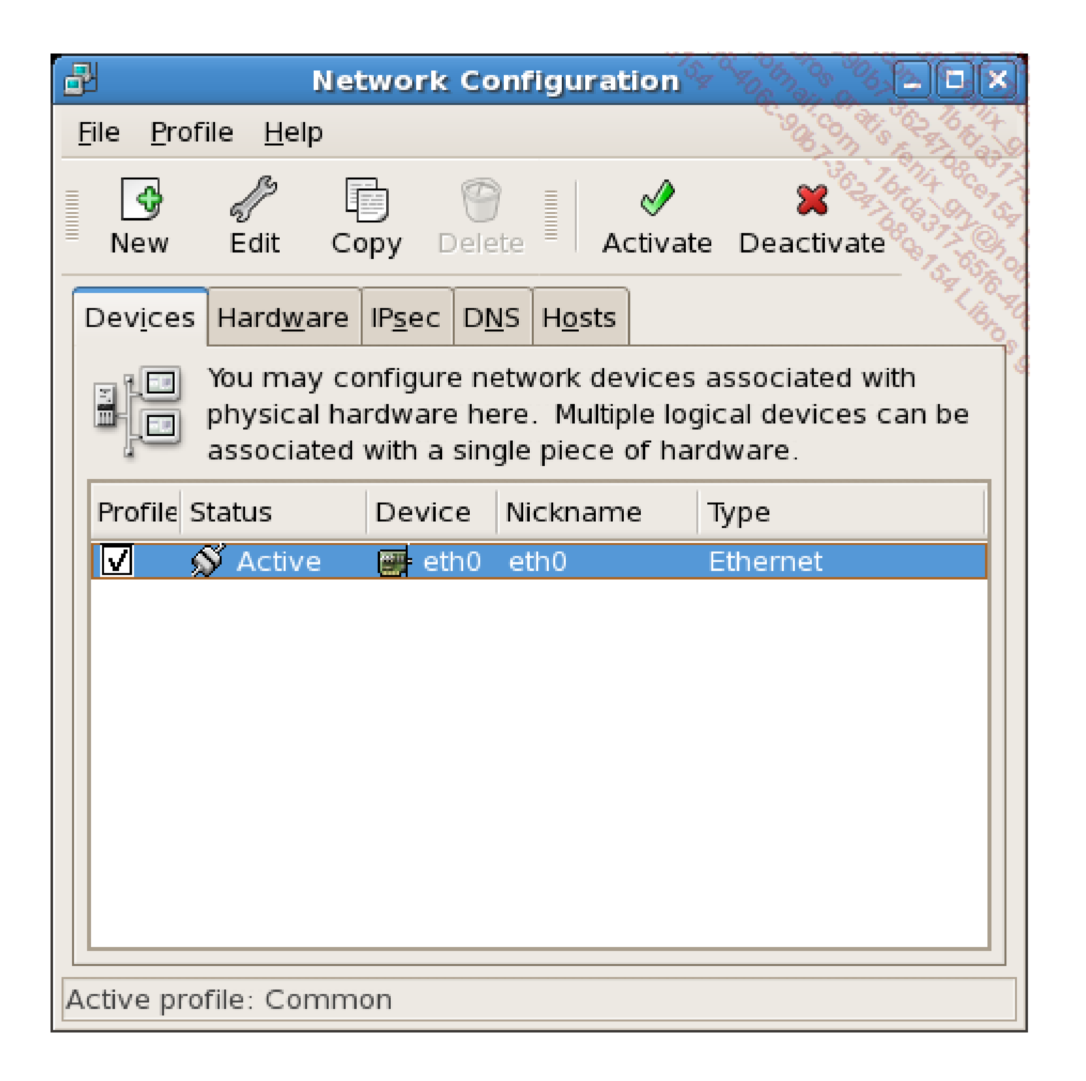
Configuración avanzada: se puede ver el tipo de controlador detectado

Durante la utilización del sistema, tras la instalación, la tarjeta se puede configurar gráficamente, como muestran las pantallas que aparecen a continuación. Vemos que se puede elegir la dirección MAC utilizada.



Propiedades de la interfaz eth0

Los cuadros de diálogo permiten activar y desactivar la interfaz o modificar el controlador, como en Windows. Si no se encuentra el controlador adecuado, es posible descargarlo de Internet, por ejemplo, del sitio del fabricante, e instalarlo.



Configuración de la interfaz eth0

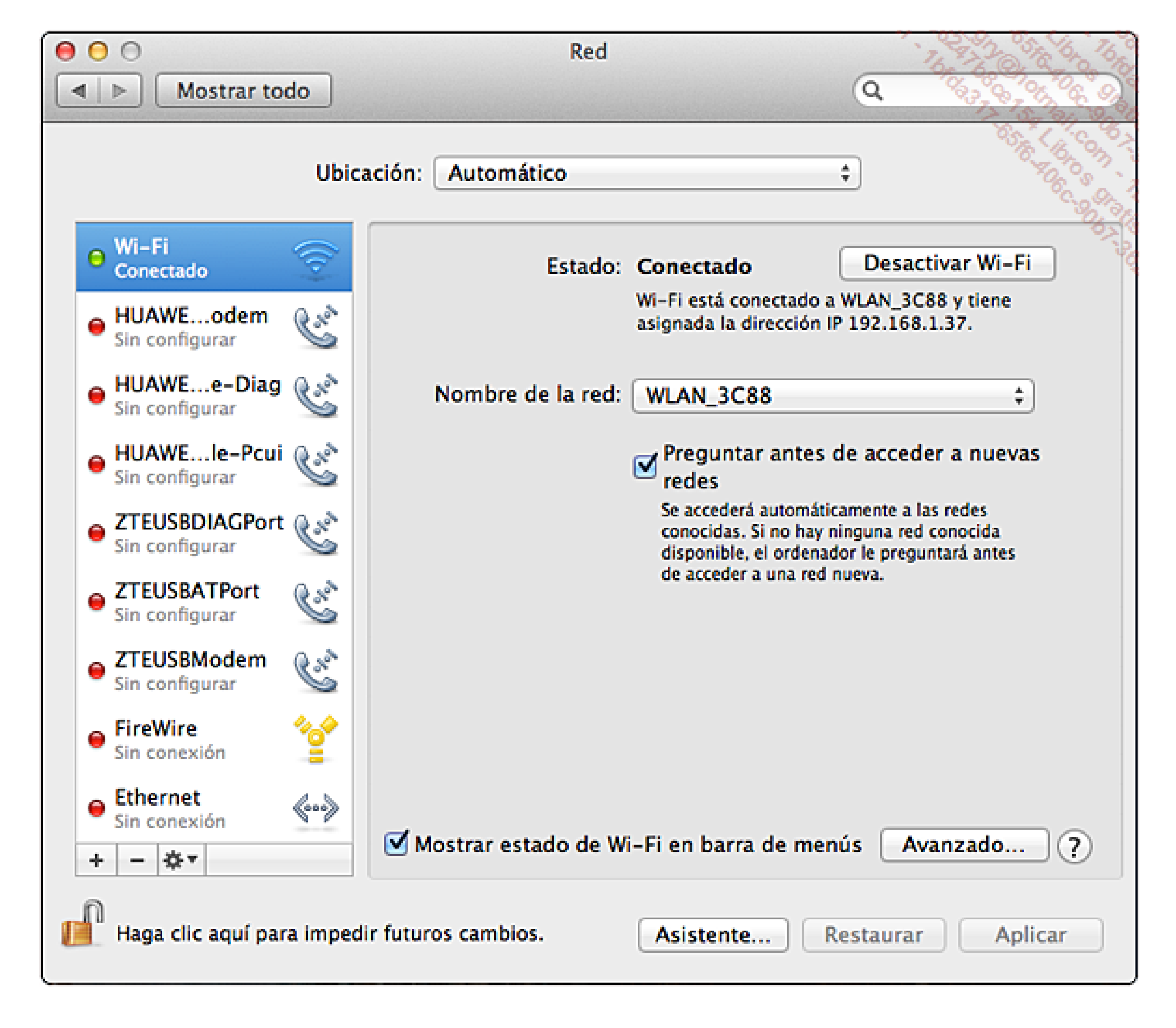
c. En un Mac OS X

Se puede acceder a la configuración de red en Mac a partir del menú **Manzana -Preferencias del sistema**:



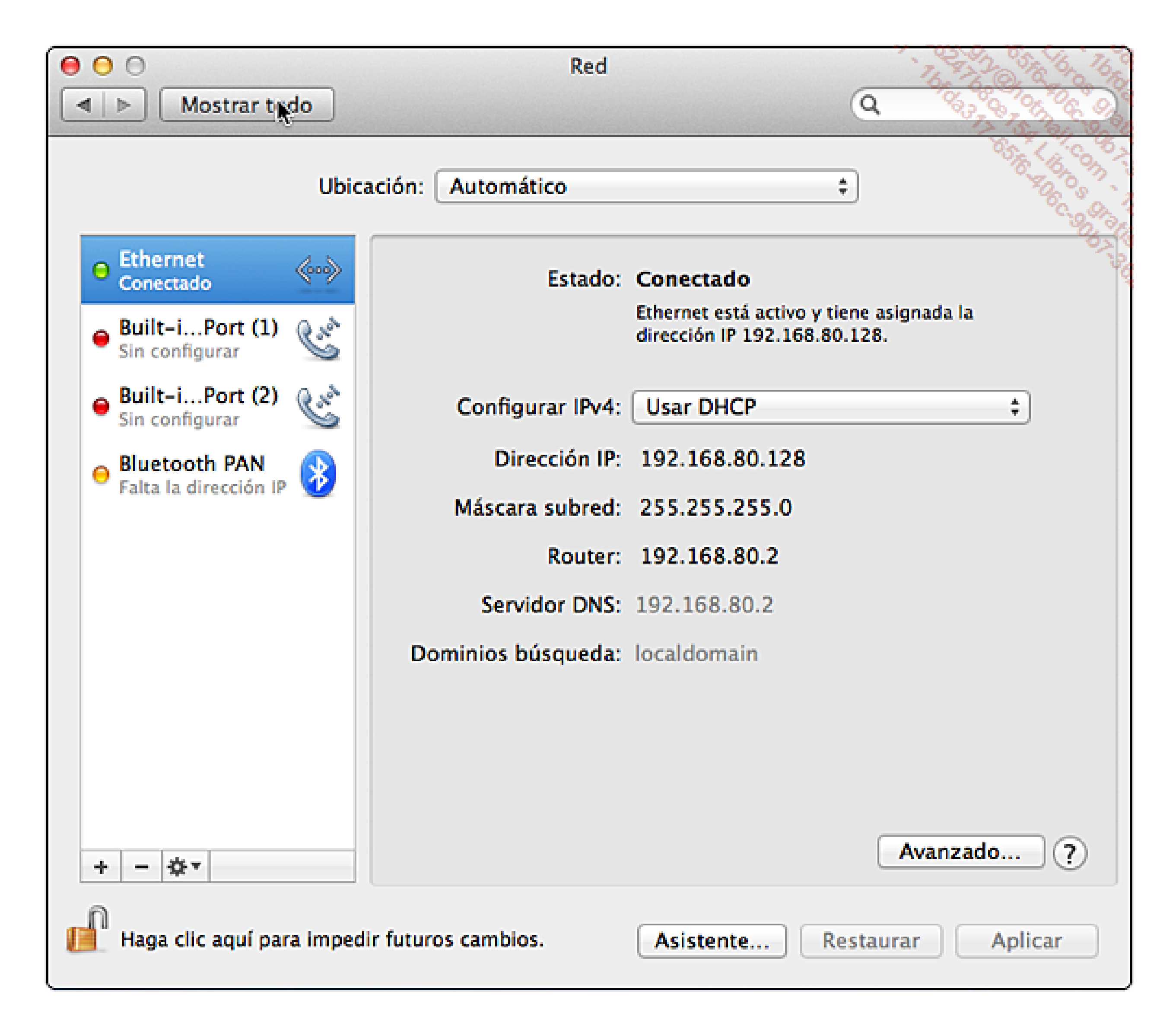
Preferencias del Sistema

- A continuación, seleccione **Red**.



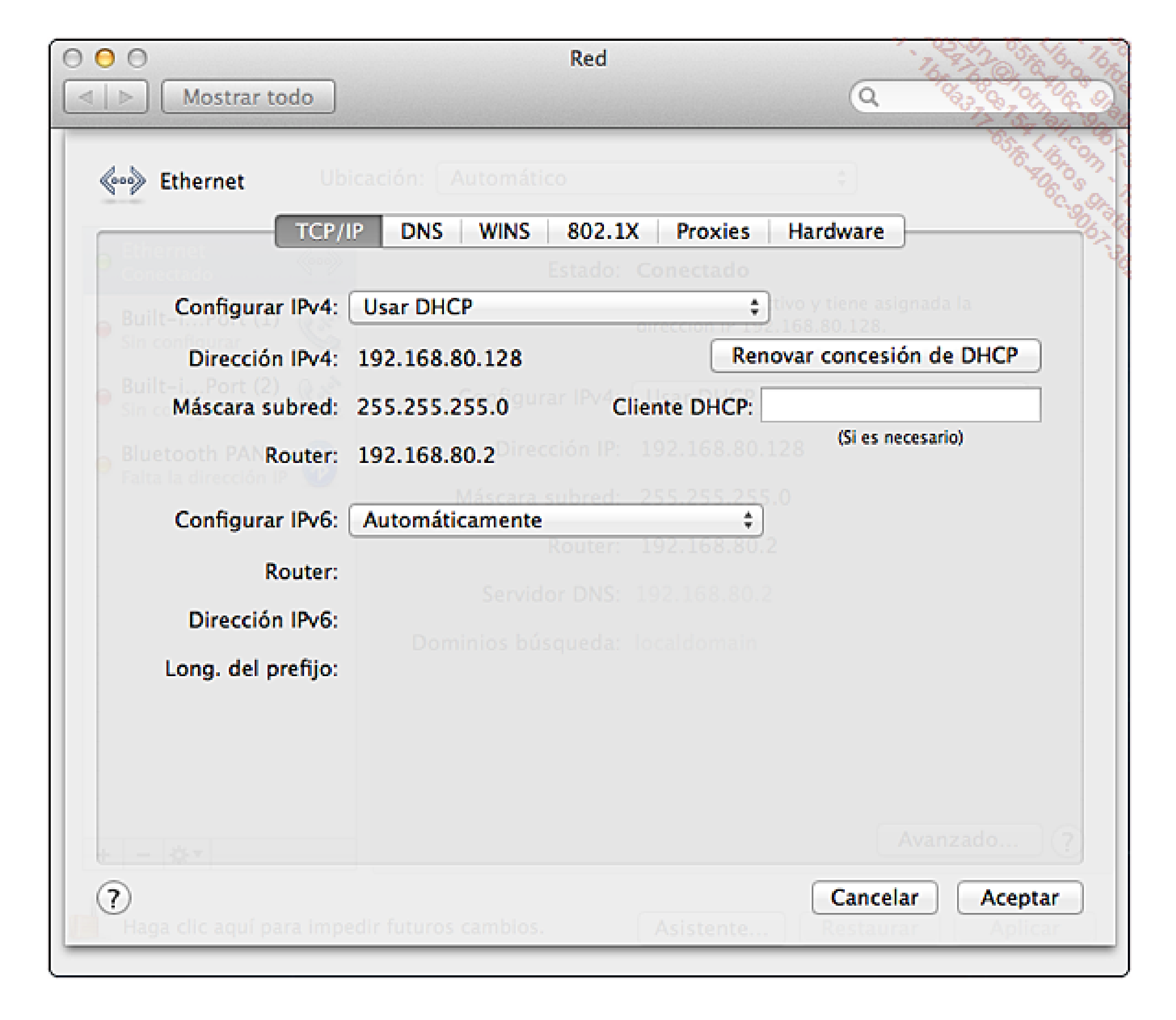
Red con conexión Wi-Fi

Cuando la red cableada está conectada, **Ethernet** aparece al principio de la lista:



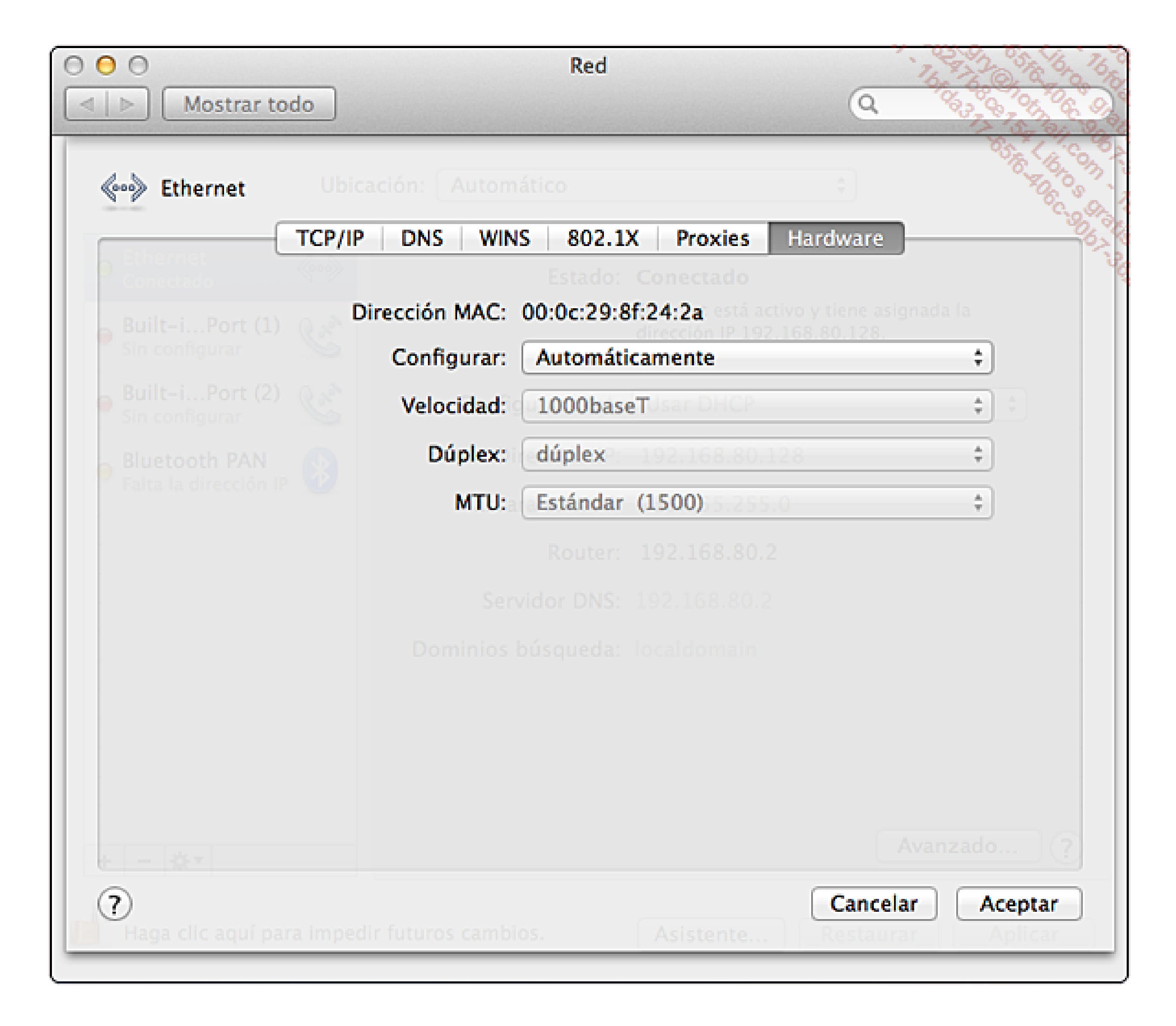
Red Ethernet

El botón **Avanzado** permite el acceso a numerosos parámetros complementarios:



Parámetros avanzados

La configuración de la tarjeta de red en sí misma está disponible a través del botón **Hardware**:



Hardware

d. En un smartphone Android

La configuración de red en un *smartphone* es mucho más breve que en un ordenador. De hecho, en el momento en que se activa la red Wi-Fi, la configuración se limita a introducir la información de autenticación.

El primer paso consiste en la activación de Wi-Fi en el *smartphone*.

- Para ello, acceda al menú **Ajustes**.



*Acceso al menú **Ajustes***

- Haga clic en **Ajustes** para que aparezca la opción **Conexiones inalámbricas y redes**.



*Acceso al menú **Conexiones inalámbricas y redes***

➜ Haga clic en **Conexiones inalámbricas y redes** para que aparezca el menú correspondiente:



Activación de Wi-Fi

➜ Marque la casilla **Wi-Fi** para activar la red inalámbrica. El teléfono buscará las redes Wi-Fi cercanas:



Selección de una red

Cuando aparezcan varias redes, puede elegir la red a la que se desea conectar.

- Si se requiere autenticación, deberá indicar la contraseña:



Introducción de una contraseña WEP

Una vez se ha introducido la contraseña, se intenta una conexión. Si todo es correcto, se asigna una IP al *smartphone*:



Obtención de una dirección IP

La selección de la red sobre la que se ha realizado la conexión permite obtener información adicional:



Ahora puede abrir un navegador de Internet para acceder a sus sitios favoritos.



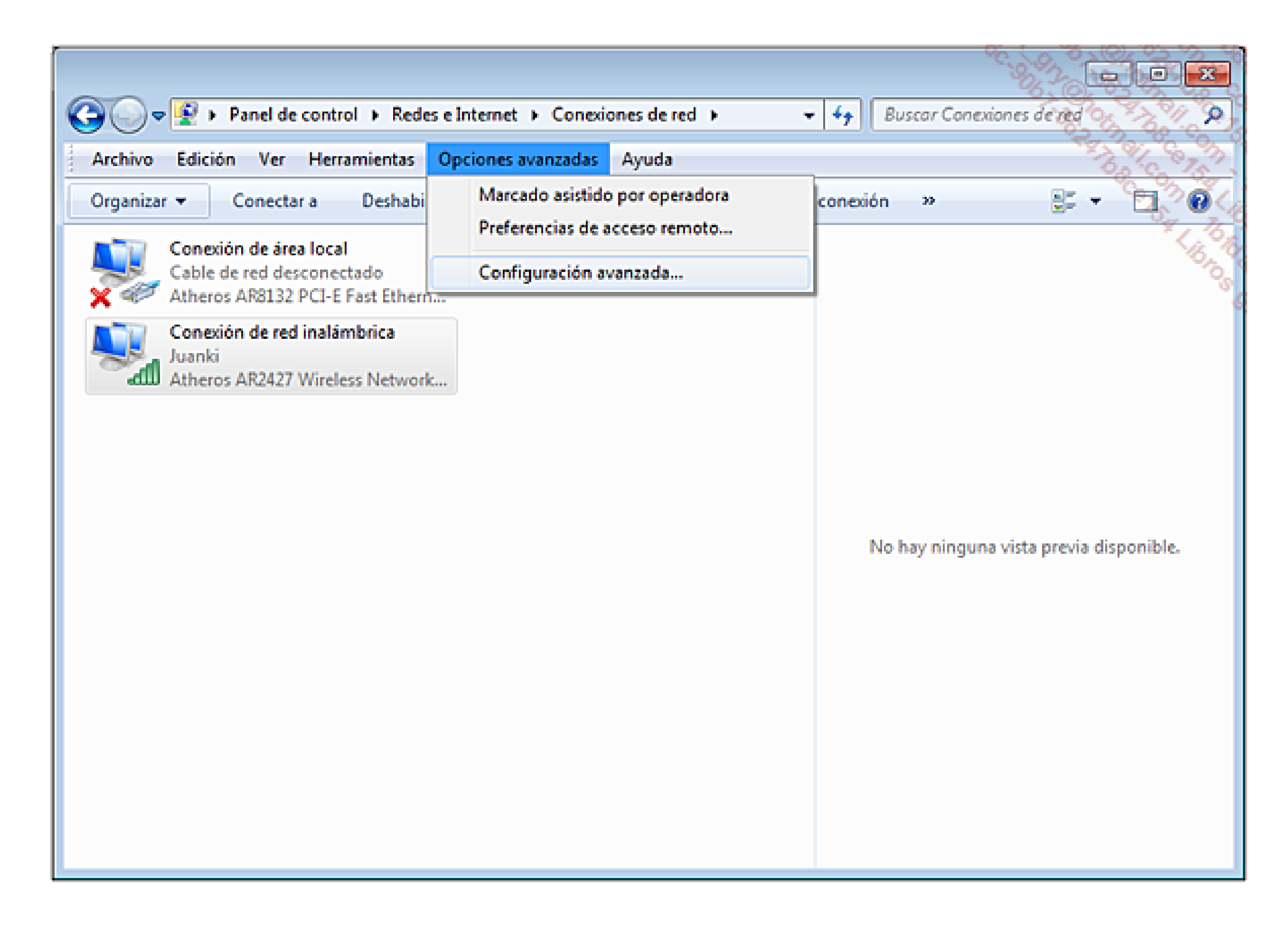
Conexión a Internet a través de Wi-Fi

Pila de protocolos

Es importante saber que, en un ordenador, es posible encontrar varias tarjetas de red, que pueden operar con diferentes protocolos, en los que se pueden ejecutar diferentes servicios. Hablaremos de pila de protocolos para designar las capas sucesivas y los vínculos que entran en juego entre las diferentes capas.

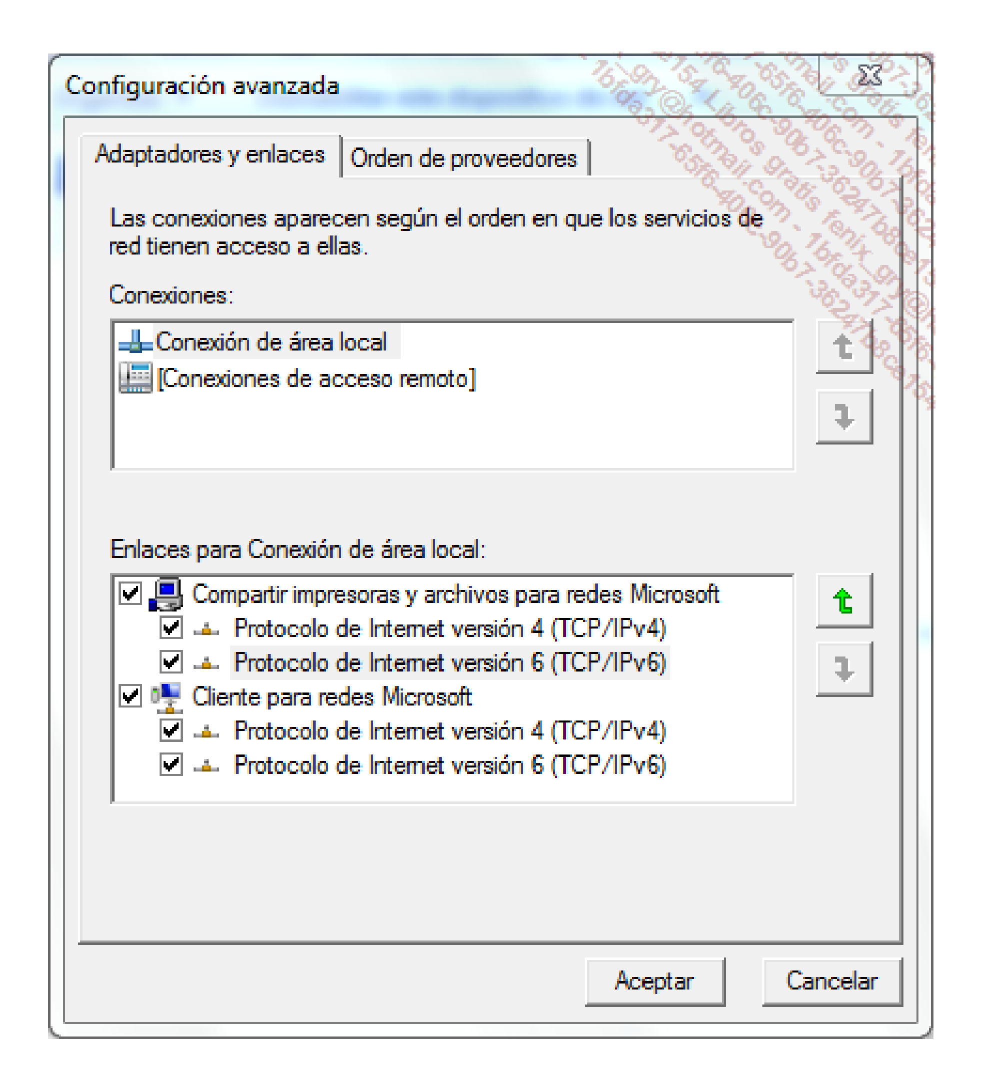
A un determinado nivel, una capa puede trabajar con otras capas inmediatamente adyacentes. Durante la configuración del modelo de red utilizado, es posible favorecer una conexión en detrimento de otra, logrando así una optimización de la configuración.

En un ordenador con un sistema operativo Windows, por ejemplo, se puede acceder a esta configuración en los parámetros avanzados de las conexiones de red.



Conexiones de red en Windows 7

En la siguiente pantalla, podemos ver que se puede dar más prioridad a una interfaz de red subiéndola respecto a otras. En la pantalla inferior del cuadro de diálogo, el **Protocolo de Internet versión 4 (TCP/IPv4)** tiene prioridad respecto al **Protocolo de Internet versión 6 (TCP/IPv6)**.



Propiedades de red en Windows 7

Detección de un problema de red

1. Conexión física de red

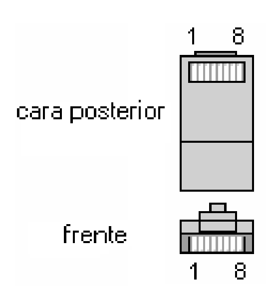
Existen diferentes causas de errores vinculados a la puesta en marcha de una tarjeta de red en un sistema operativo. Vamos a ver cuáles son las más habituales y las acciones que hay que emprender para resolver el problema.

a. El tipo de cable

Es importante tener en cuenta el tipo de cable correcto, normalmente de cobre. Incluso si los conectores RJ45 parecen iguales, algunos se han adaptado específicamente para algunas velocidades y tienen que corresponder a la categoría de cable utilizada. Igualmente, se debe certificar la interconexión para una categoría dada, y no basta con disponer de cables y de conectores de categoría 5; el trabajo se debe hacer correctamente.

La conexión directa entre dos ordenadores se debe realizar con un cable cruzado. La conexión de un ordenador a una toma de red o a un concentrador (o cualquier otro elemento similar) se debe realizar con un cable directo.

- Verifique que dispone de un cable directo cuando se conecta a un *hub* (para ello, observe los hilos de colores utilizados en los dos extremos de los conectores RJ45).
- Verifique que dispone de un cable cruzado cuando se conecte directamente a otro equipo (de tarjeta de red a tarjeta de red).



Así, para un **cable directo**, el código de color adoptado será el siguiente en cada uno de los conectores (ej. norma T568B):

1	Blanco-Naranja	5	Blanco-Azul
2	Naranja	6	Verde
3	Blanco-Verde	7	Blanco-Marrón
4	Azul	8	Marrón

Para un **cable cruzado**, uno de los extremos adoptará el siguiente orden:

1	Blanco-Verde	5	Blanco-Azul
2	Verde	6	Naranja
3	Blanco-Naranja	7	Blanco-Marrón
4	Azul	8	Marrón

La unión de los hilos se explica en el capítulo Transmisión de datos en la capa física - El conector RJ45.

b. El tipo de componentes

Cuando conecte una tarjeta de red a un concentrador con un cable de par trenzado directo, hay que verificar que el puerto utilizado no es cruzado (Up Link).

Muchos equipos de nueva generación, como los conmutadores, pueden detectar si el cable es directo o cruzado y adaptarse en consecuencia.

Compruebe las características del componente:

- Tipo de red de nivel 2 OSI soportada: Token Ring, Ethernet; las dos pueden utilizar cables con conectores RJ45.
- Velocidad soportada (ejemplo 10/100 Mbps para la tarjeta de red, pero solo 10 Mpbs para el elemento activo).

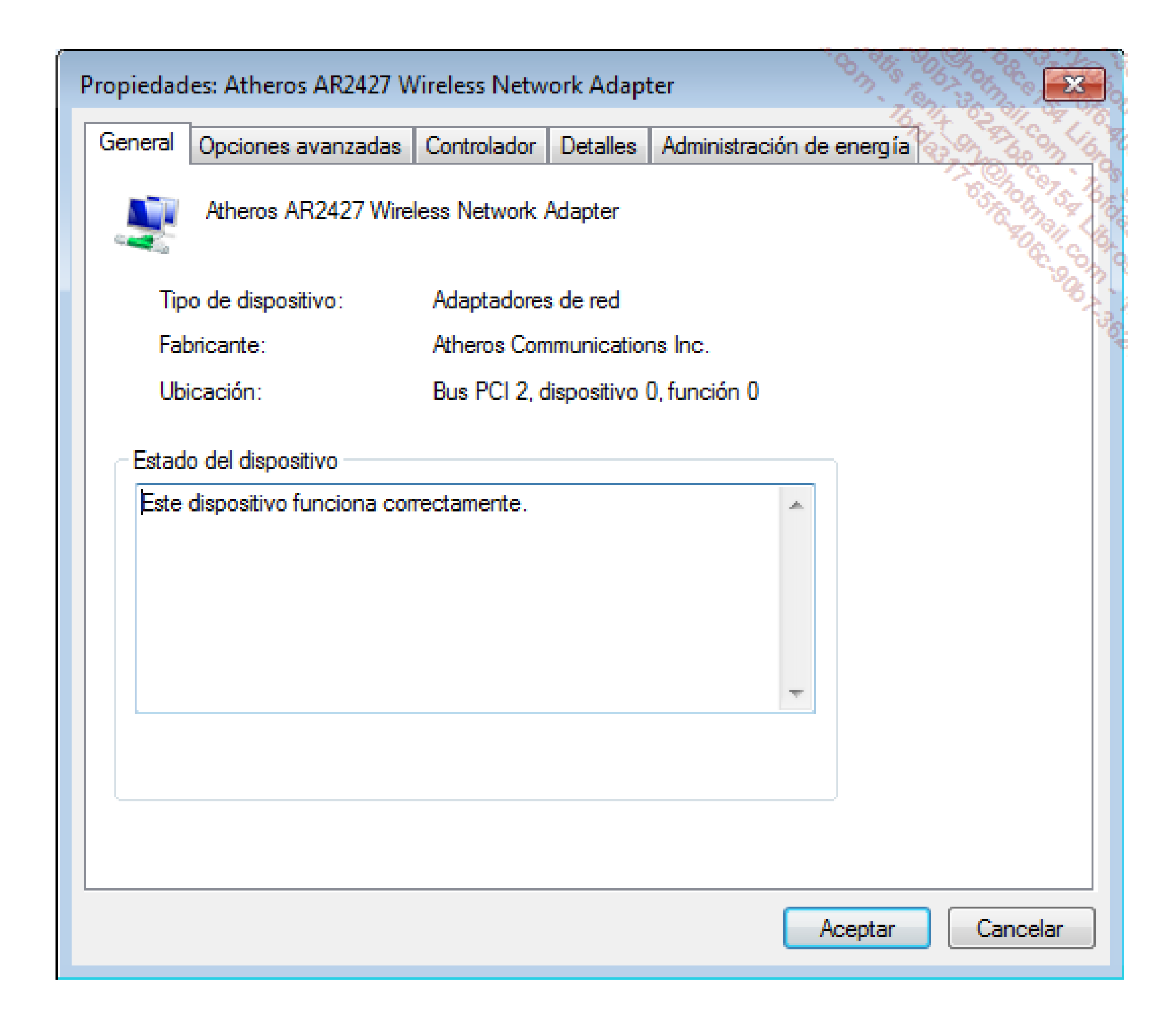
Si conecta el ordenador a una toma de red, no olvide comprobar, o hacer comprobar, que está bien conectada y que está conectada a un equipo de red.

2. Configuración del software de red

Con la generalización de las interfaces de red detectadas automáticamente, el problema del mal funcionamiento debido a la configuración del software es mucho menor.

En la actualidad, es muy raro tener que configurar manualmente la tarjeta, con la ayuda de herramientas del fabricante o integradas en el sistema operativo. Sin embargo, puede ser necesario hacer ajustes más precisos en las interfaces de servidores, como forzar una velocidad concreta o el modo de comunicación (*half* o *full duplex*).

La mayoría de las veces, es el mismo controlador el que puede causar un problema de software. Puede ser necesaria la instalación de una versión más reciente. En cambio, algunos controladores demasiado recientes no son implementados correctamente por el sistema operativo o son defectuosos. En este caso, se recomienda probar la tarjeta con un controlador más antiguo certificado por el sistema operativo.



Propiedades de una tarjeta de red en Windows

Topologías

Una topología caracteriza la forma en que se organizan los distintos equipos de una red para interactuar entre ellos.

1. Principios

Se distingue entre la topología física, en relación con el plano de la red, y la topología lógica, que identifica la forma en que la información circula por el nivel más bajo.

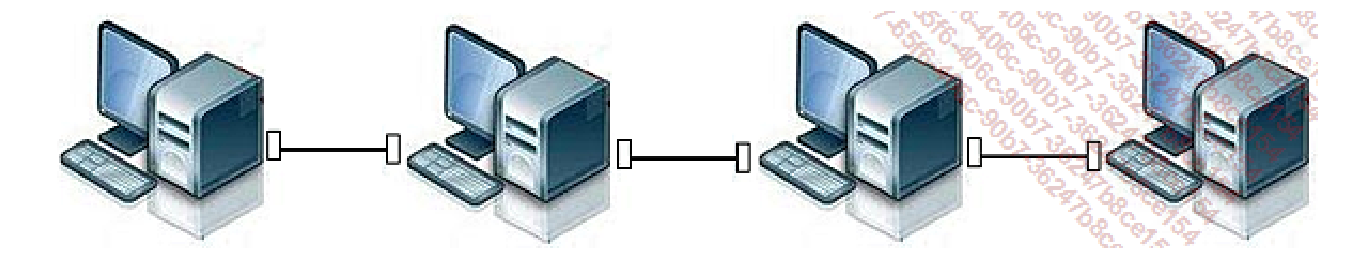
La interconexión entre nodos de la red se realiza en forma de conexión punto a punto, es decir, uno a uno, o en forma de multipuntos, n nodos con n nodos.

2. Topologías

a. El bus

La topología en bus (soporte lineal) se basa en un cableado en el que se conectan los nodos (puestos de trabajo, equipos de interconexión, periféricos). Se trata de un soporte multipuntos. El cable es el único elemento físico que constituye la red y solo los nodos generan señales.

La cantidad de cables utilizados es mínima y no se requiere un punto central. El inconveniente principal recae en el hecho de que un corte del cable en solo un punto impide que cualquier equipo pueda intercambiar información a través de la red.

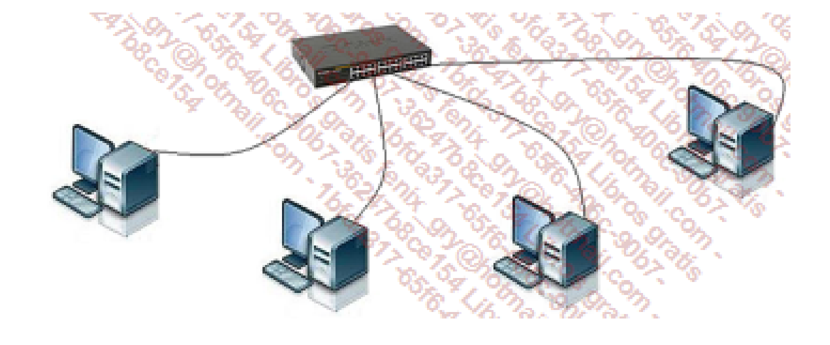


Topología en bus punto a punto

b. La estrella

La topología en estrella descansa, por su parte, en componentes activos. El componente activo restablece y regenera las señales. Integra una función de repetidor.

Estos puntos centrales se llaman *hubs*. Es posible crear una estructura jerárquica creando un número limitado de niveles.

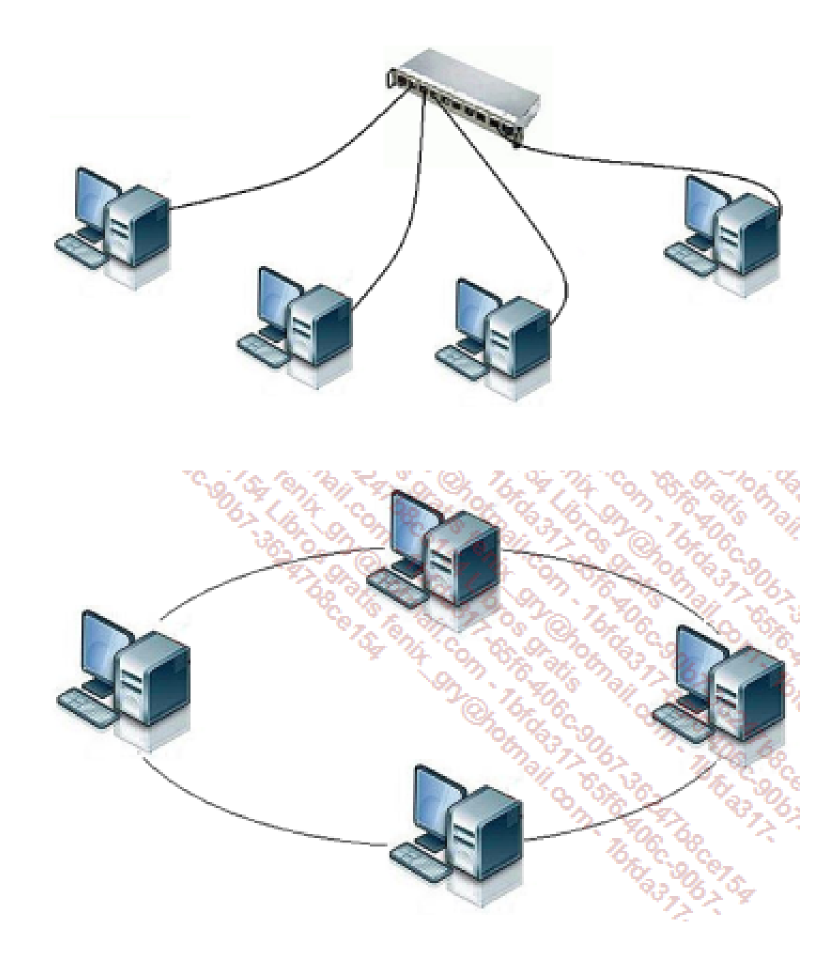


Topología en estrella

La utilización de un *hub* en una red Ethernet crea una topología física de estrella, aunque consideremos que su topología lógica es en bus.

c. El anillo

Esta topología se basa en un bucle cerrado, un anillo (*ring*), que comprende conexiones punto a punto entre los dispositivos. Las tramas transitan por cada nodo, que se comporta como un repetidor (elemento activo). Los *hubs* en anillo permiten insertar equipos en la red. Contienen no solo puertos para estas, sino también dos conectores macho/hembra denominados R/I (*Ring In*) y R/O (*Ring Out*) para realizar los bucles entre elementos. Permiten conexiones de cables de cobre (RJ45) o de fibra. Se diferencia entre MAU (*Multistation Access Unit*), pasivo, y CAU (*Controlled Access Unit*), activo.

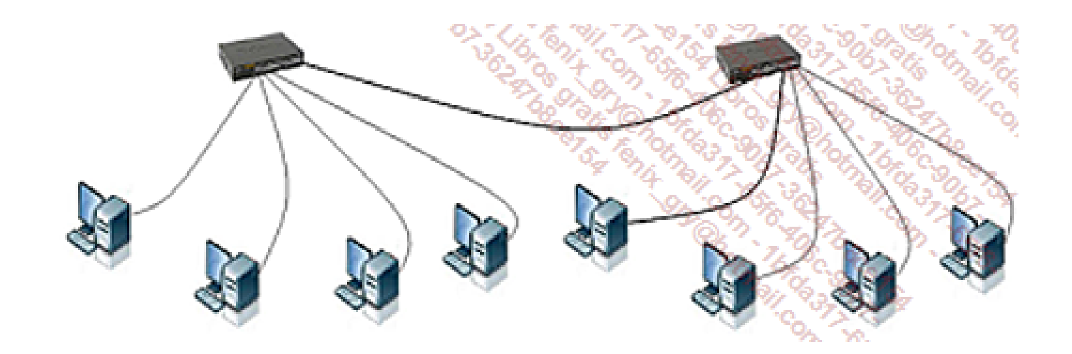


La utilización de un MAU en una red crea una topología física en estrella, mientras que la lógica es en anillo.

Aunque el Token Ring cada vez se utiliza menos, es interesante entender bien este tipo de topología.

d. El árbol

En la estructura en árbol, los equipos se conectan de manera jerárquica entre ellos, por medio de *hubs* en cascada (*stackable hubs*). Esta conexión debe ser cruzada.



Topología en árbol o estrella jerárquica

En Ethernet con par trenzado, es posible interconectar hasta cuatro niveles de *hubs*.

e. Las topologías derivadas

Enmallado

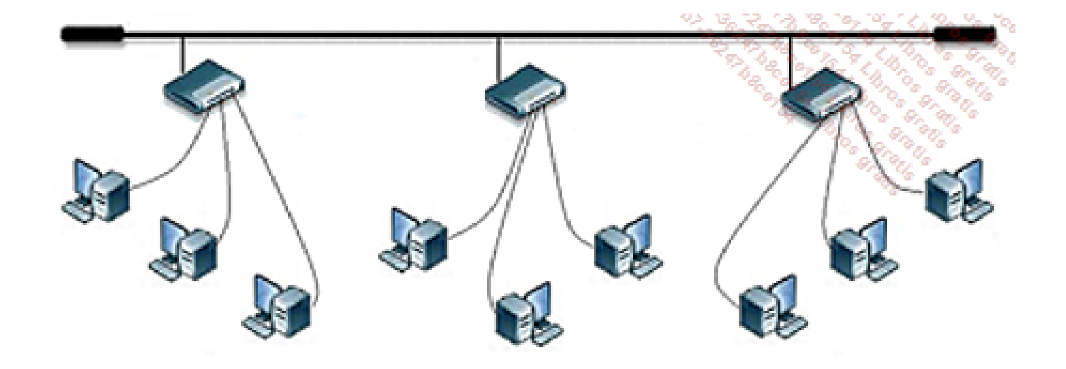
Hablaremos de una red en malla para referirnos a una arquitectura constituida por topologías mixtas, como Internet (red extendida mundialmente o *World Wide Web*).

La interconexión punto a punto, mediante módems, por ejemplo, de dos sitios estructurados con una topología particular cada uno constituye una red híbrida.

Bus en estrella

Los elementos activos de la red, en los que se conectan las estaciones de trabajo, pueden estar conectados entre sí en bus.

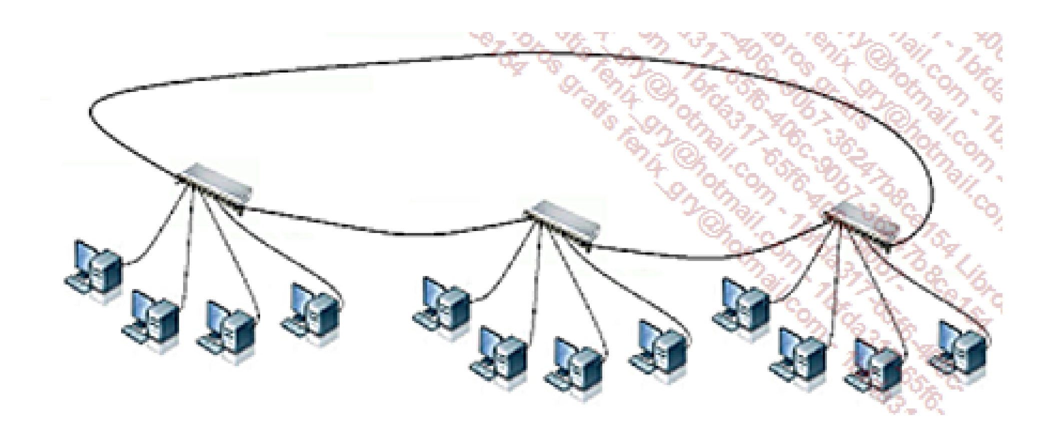
Varios *hubs* conectados entre sí mediante una red troncal (a menudo de fibra óptica) forman una red con topología de bus en estrella.



Topología bus en estrella

Anillo en estrella

Se habla de anillo en estrella cuando se conectan varios anillos entre ellos.



Topología anillo en estrella

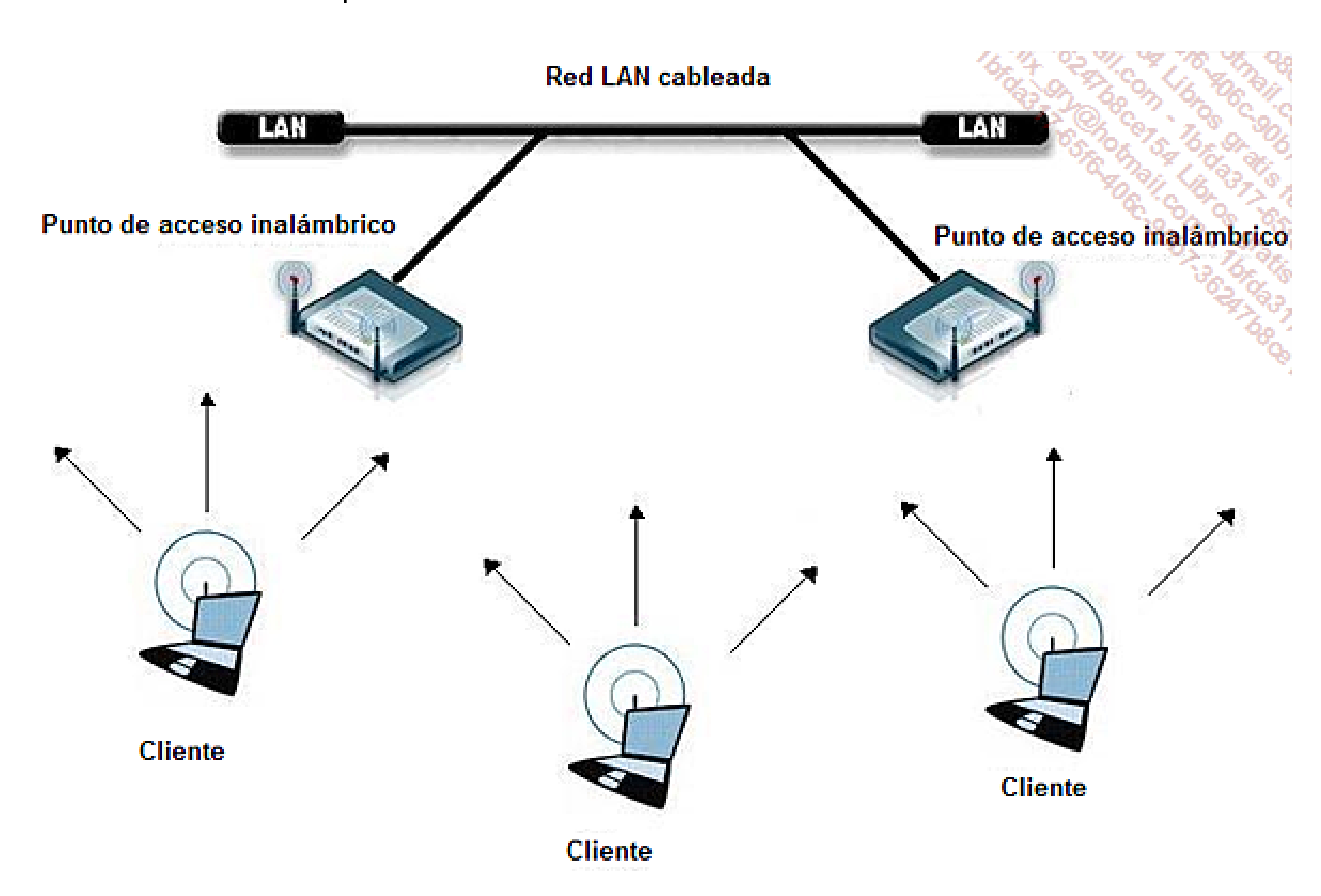
f. El caso de las redes inalámbricas

Conexión punto a punto

A través de una interfaz de red inalámbrica se pueden comunicar directamente dos nodos. También se le llama conexión de tipo punto a punto (*peer to peer*) o *ad hoc*. Una configuración como esta es posible con las tecnologías Bluetooth o Wi-Fi.

Conexión multipuntos

Un componente centralizador, como el punto de acceso (AP - *Access Point*) y Wi-Fi centralizan las comunicaciones. También permiten la interconexión con la red cableada local.



Las nuevas tecnologías de redes inalámbricas auguran un uso de tipo de red en malla (*mesh*), cuyas estaciones de trabajo podrán retransmitir la comunicación a múltiples puntos.

Elección de la topología de red adaptada

No hace tanto tiempo, se planteaba la cuestión de elegir entre las topologías en bus, en estrella o en anillo.

En ocasiones todavía encontramos esta última, pero son raros los diseños de red modernos que utilizan este tipo de red. Podemos encontrar el bus en las redes industriales.

Las redes locales de oficina ya están estandarizadas, tanto en los protocolos utilizados como en las topologías. Lo normal es la red en estrella, con una conexión directa de las estaciones de trabajo y los servidores a los *hubs*. Estos *hubs* están conectados entre sí, a menudo por buses de fibra óptica. Esta topología permite organizar una red productiva a un precio razonable.

Gestión de la comunicación

La circulación de la información a través de la red, el tipo de transmisión y el compartir los medios de comunicación son aspectos importantes de la arquitectura.

1. Dirección del flujo de información

Hay muchas direcciones o sentidos posibles para la gran cantidad de datos que circulan en una red, que dependen, sobre todo, del soporte de transmisión y de las tecnologías utilizadas.

a. El modo simplex

Este modo solo utiliza un único sentido de transferencia de información. Generalmente hay un único emisor, al que corresponden n receptores, que además son poco costosos.

La emisión de programas de radio es un ejemplo de utilización de comunicaciones en modo simplex.

La fibra óptica ofrece solo un sentido de transmisión, permitiendo únicamente el modo*simplex*. Por ello, para posibilitar una comunicación bidireccional, se deben utilizar al menos dos fibras.

b. El modo half-duplex

Cada interfaz es, a la vez, emisora y receptora. Se alternan los dos sentidos de comunicación.

Las radios de aficionados (CB - *Citizen Band*) se basan en este modo.

El cable coaxial es un buen ejemplo de soporte *half-duplex*.

c. El modo full-duplex

En este modo, los dos extremos pueden transmitir simultáneamente. Es la solución más costosa, pero también la más eficaz.

Las comunicaciones telefónicas son de tipo full-duplex.

El soporte en cable de par trenzado es un medio de comunicación de transmisión *full-duplex*. Una tarjeta de red conectada al equipo adecuado puede utilizar simultáneamente un par de hilos para la emisión y otro par para la recepción.

2. Tipos de transmisión

Los datos transmitidos deben ser sincronizados por el receptor para leerlos. Para ello se pueden utilizar varios tipos de transmisión. Los principales son:

- Síncrona, utiliza un reloj para transmitir flujos continuos.
- Asíncrona, permite administrar un intercambio no previsto u ocasional, comenzando por un bit de inicio (*start*) y terminando por un bit de parada.
- Isócrono, en el que se fija la periodicidad, pero independientemente de ningún reloj, para dar

una señal continua.

En las redes locales, se utilizan especialmente los dos primeros tipos. La siguiente tabla muestra sus características con más detalle.

	Síncrona	**Asíncrona**
Ventajas	Más eficaz. Alta velocidad. Mejor detección de errores.	Sencilla. Material barato.
Inconvenientes	Los circuitos de emisión y recepción son más complejos y más caros.	La asignación a trama de cada carácter y la detección de los errores corresponde a un 20 o 30 % de la velocidad útil. El bit de paridad solo detecta un error. Transferencia lenta.

3. Métodos de acceso al soporte

En un canal punto a punto, un emisor puede transmitir libremente. En cambio, cuando el soporte es compartido por varios periféricos, es necesario administrar la forma en que se intercambian datos.

Estos intercambios dependen de la arquitectura de red, es decir, de la topología lógica.

Un modo de acceso define las normas que regulan el acceso a cada componente, la transmisión y la liberación del canal compartido. Se distinguen esencialmente tres modos: el de contención, el *polling* y el paso de testigo.

a. La contención

En el modo de acceso por contención, cada equipo emite cuando lo necesita, después de escuchar el canal o el portador (CS - *Carrier Sense*), que debe estar disponible. Se escucha la trama emitida para comprobar que ninguna señal perturba la emisión. Es este caso no hay ningún arbitraje del canal.

Dos equipos pueden emitir simultáneamente, lo que puede conducir a una sobretensión en el caso de un cable coaxial, o a una recepción de información sobre el par receptor mientras se emiten algunos datos sobre el otro par (par trenzado). Este estado se denomina de colisión, y es necesario detectarlo.

Estas situaciones ocurren si respetamos algunas de las condiciones (por ejemplo, el alcance máximo de la red). Por ello, con Ethernet, el tamaño de una trama no debe ser inferior a 64 bytes, de manera que el equipo emisor sea capaz de detectar la colisión antes de haber enviado el último byte de la trama.

Como dato orientativo, un bit de dato de una trama en Ethernet de 10 Mbps está representado por una señal que se extiende sobre 23 metros. Lo que implica que la trama más pequeña Ethernet (de 64 bytes) puede tener una extensión de 10 km.

Cuando se produce una colisión, el primer equipo que lo detecta prolonga su emisión a través de una señal especial (trama de interferencia o JAM), con el fin de avisar a los otros equipos de que hubo una colisión.

En este caso, se define aleatoriamente un tiempo de espera para cada equipo que emitía en el momento de la colisión. Así no intentarán reanudar el control del canal en el mismo momento.

Las dos implementaciones más extendidas de la contención son CSMA/CD y CSMA/CA.

CSMA corresponde a la escucha del portador (*Carrier Sense*) en un soporte compartido (*Multiple Access*). Las dos implementaciones se distinguen por el hecho de que una detecta las colisiones (*Collision Detection*) y la otra intenta evitarlas (*Collision Avoidance*).

El segundo caso es una alternativa con relación al modo anteriormente mencionado. De hecho, en vez de intentar transmitir los datos arriesgándose a una colisión (después de escuchar el soporte), el dispositivo envía una trama preliminar para informar a los otros equipos de que quiere utilizar el canal (para enviar su trama de datos).

CSMA/CD corresponde a la implementación Ethernet, mientras que CSMA/CA es la adoptada por la norma 802.11 (Wi-Fi).

La principal ventaja de esta gestión de soporte es su simplicidad. Sin embargo, el método no es determinista, ya que el tiempo de acceso al canal no es previsible. Además, no hay gestiones de prioridad posibles para dispositivos que necesitan acceder rápidamente al soporte compartido.

b. La pregunta (polling)

Con este método se designa a un equipo de la red como administrador del acceso al canal. Este hardware, que es el supervisor, pregunta en un orden predeterminado a cada uno de los nodos si tienen información para transmitir. A menudo, el supervisor es un *hub* o *switch* y el hardware secundario son los nodos de la estrella.

La ventaja de este método es que se centralizan todos los accesos al canal. Además, el tiempo de acceso y el volumen de datos manejado en este soporte son previsibles y fijos.

Sin embargo, utiliza una parte del ancho de banda de la red para emitir mensajes de gestión (preguntas, advertencias, entregas...), lo que implica un mayor coste de ancho de banda.

c. El paso de testigo

En el método del paso de testigo, las tramas van pasando de equipo en equipo, y cada uno de estos se comporta como un repetidor. Inicialmente, una pequeña trama, el testigo (*token*), se repite de equipo en equipo hasta que una máquina que desee emitir lo conserva durante un tiempo determinado. Este método de acceso se utiliza generalmente en arquitecturas de anillo (*ring*).

Este testigo es, por decirlo de algún modo, un mensaje de autorización que ofrece la exclusividad del soporte a la estación que lo posee. Esta emite una trama que se repetirá en cada estación hasta dar la vuelta al anillo. A su paso, el destinatario de la trama, que ve pasar la señal, realiza una copia, si no es errónea y si dispone de suficiente espacio en el*buffer* de recepción. El destinatario marca la trama copiada con el fin de informar al emisor de que se ha leído.

Después de haber dado la vuelta al anillo, el emisor retira la trama, que libera al testigo dejándolo disponible para el próximo equipo.

El paso de testigo aplica una solución determinista que permite un buen control del soporte. La velocidad máxima real alcanzada es mucho más elevada que con el método de contención, propenso a las colisiones.

Hay varias normas de paso de testigo para las topologías de anillo (IEEE 802.5, Token Ring o FDDI), pero también para las topologías de bus (IEEE 802.4). Todavía se encuentran redes que implementan Token Ring o FDDI.

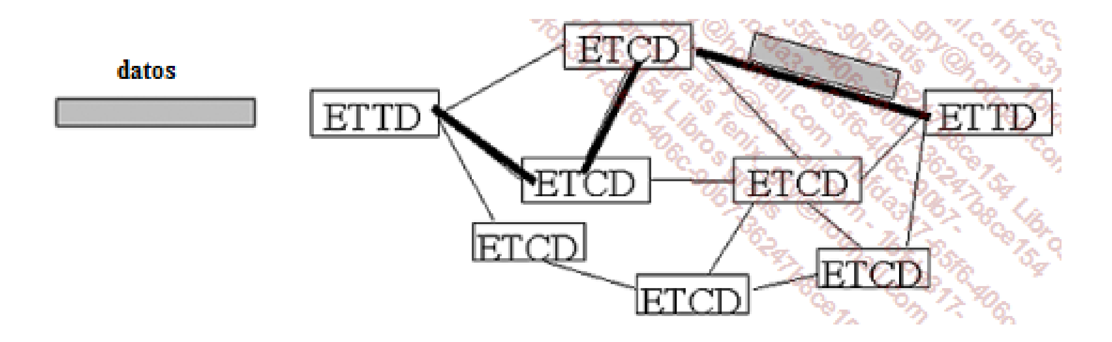
La tecnología del paso de testigo requiere un mecanismo de gestión de sistema más avanzado que el de la contención. Pero es más eficaz en las redes con una carga importante, por tanto más propensas a las colisiones. Por ejemplo, elegimos un nodo como supervisor para, entre otras cosas, generar un nuevo testigo en caso de perderlo.

4. Tecnologías de conmutación

a. La conmutación de circuitos

Este tipo de conmutación establece una conexión física temporal mientras dura el proceso de comunicación.

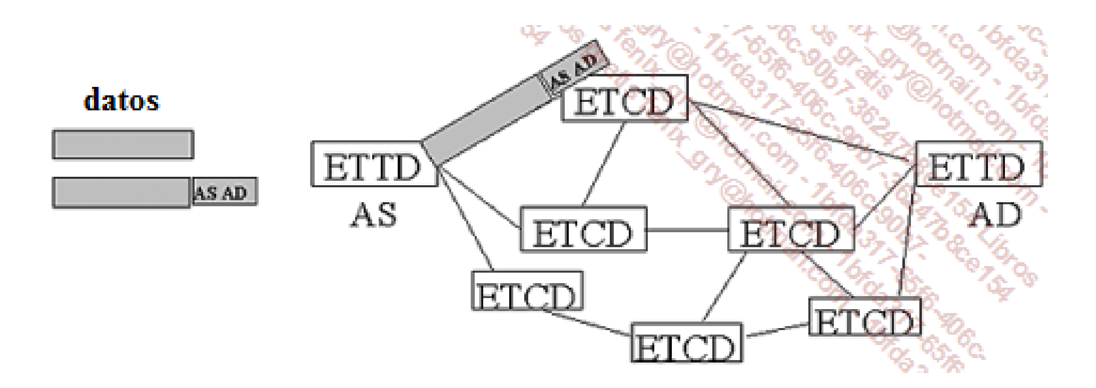
La conmutación de circuito se utiliza en la red telefónica conmutada (RTC).



Conmutación de circuito

b. La conmutación de mensajes

Con este tipo de conmutación no es necesario establecer una ruta dedicada entre los dos equipos que se comunican. En realidad, cuando un equipo envía un mensaje, la dirección del destinatario se añade al paquete. Entonces el mensaje se transmite en un solo bloque de nodo en nodo. Cada nodo recibe el mensaje completo, lo almacena unos instantes y luego lo transmite al siguiente nodo: es lo que se llama *store and forward*.



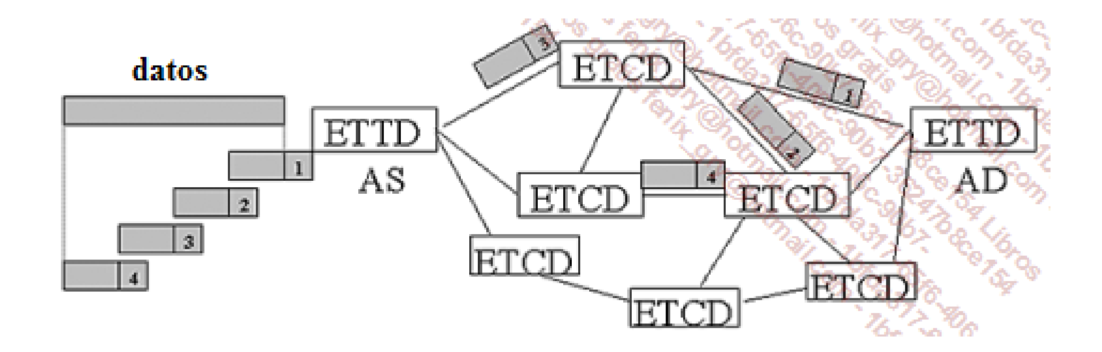
Conmutación de mensajes

c. La conmutación de paquetes

La conmutación de paquetes combina la de mensajes y la de circuitos. Se utilizan generalmente dos técnicas. En los dos casos se divide un mensaje en paquetes, cada uno de los cuales contiene las direcciones de origen y de destino.

Datagrama

En la conmutación de paquetes por datagrama, cada datagrama sigue su propio camino (en el sentido de la conmutación de mensajes). Por lo tanto, además de la dirección del destinatario, es necesario numerar en secuencia los datagramas, con el fin de volver a poner en orden los paquetes reconstruyéndolos como mensajes a la llegada. De hecho, como un datagrama sigue su propio camino, puede que llegue antes que otro emitido con anterioridad.

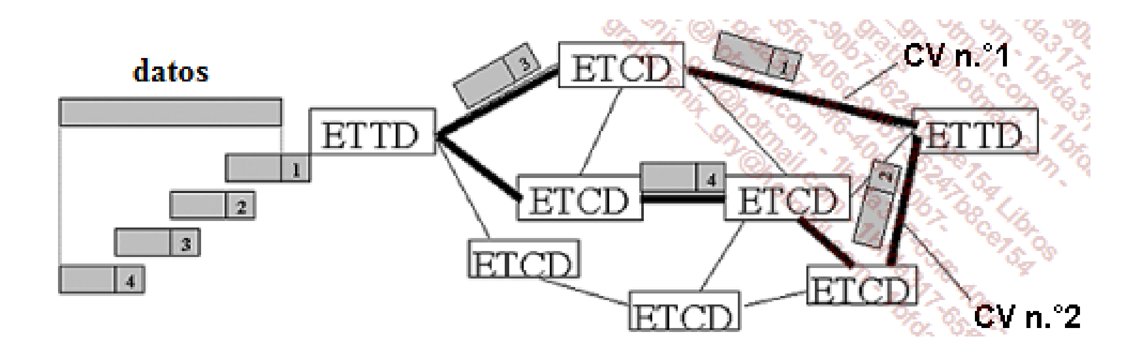


Conmutación por datagramas

Circuito virtual

Los circuitos virtuales (CV) requieren el establecimiento de conexiones lógicas entre el emisor y el receptor. Se establece una conexión lógica al principio de un intercambio con el fin de decidir todos los parámetros inherentes a la comunicación: la elección del camino, el tamaño del paquete, las entregas necesarias, el control de flujo, la gestión de errores. Los circuitos virtuales permiten la asignación por demanda del ancho de banda.

Esta técnica se estandarizó como X.25.



Conmutación por circuitos virtuales

Interconexión de redes

Cada topología tiene sus límites en términos de longitud máxima del segmento, número de equipos por segmento, etc. Una de las necesidades actuales es la de aumentar el número posible de equipos de red o interconectar redes del mismo tipo (topología, modo de acceso) o de tipos diferentes.

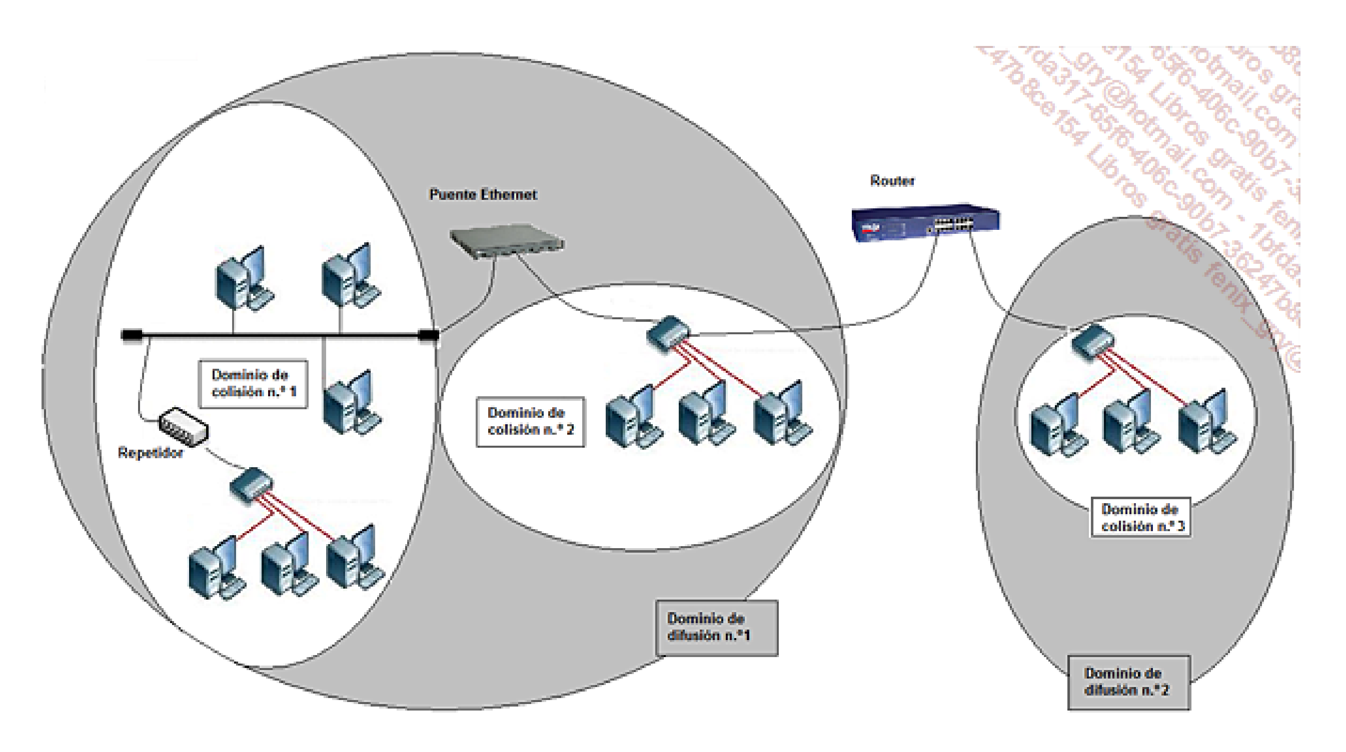
1. Principios

Existe hardware que permite interconectar las redes entre ellas. También permite segmentar las redes de gran tamaño en sectores más manejables.

En una red Ethernet, por ejemplo, el dominio de colisión se refiere a la extensión máxima que alcanza la trama en una red física.

En Ethernet, el hecho de dividir una red en dos dominios de colisión por medio de un puente permite desatascar la red.

Usaremos la expresión dominio de difusión para identificar las partes de la red sobre las cuales una trama física, cuya dirección MAC es una dirección de difusión (es decir, FF.FF.FF.FF.FF.FF), puede extenderse. Puede ser interesante reducir los dominios de difusión a través de routers, debido a que algunos servicios trabajan solamente por medio de difusiones.



2. Componentes de interconexión y modelo OSI

En primer lugar, es muy importante comprender la relación que existe entre el modelo OSI, TCP/IP y los componentes de interconexión de red.

Según el nivel de funcionamiento de cada componente, podemos distinguir entre los que se basan en la dirección MAC y los que utilizan la dirección IP para filtrar los accesos.

	Modelo OSI				Modelo TCP/IP
7	Aplicación		Puerta de enlace		Aplicación
6	Presentación				
5	Sesión				
4	Transporte				Transporte
3	Red	Router		Dirección IP	Internet
2	Conexión	Puente, *Switch*		Dirección MAC	Interfaz de red
1	Física	Repetidor, *hub*, tarjeta de red			

Los conmutadores más avanzados son capaces de manejar los datos en la capa Red, a pesar de no ser esta su función original.

3. Descripción funcional de los componentes

a. El repetidor

Un repetidor (*transceiver*) actúa en la capa física del modelo OSI. Vuelve a empaquetar los datos recibidos y los retransmite con el fin de aumentar la distancia de transmisión. Es necesario transformar la señal en datos y luego los datos en señal, ya que las señales digitales son propensas a una atenuación muy marcada.



Repetidor fibra/par trenzado

Las señales cuadradas tienen una incontenible tendencia a perder amplitud (deteriorarse) y triangularse.

Un repetidor actúa en un mismo soporte físico, salvo si el repetidor asume la interconexión de soportes heterogéneos.

El repetidor no tiene ninguna información de la semántica de los campos de la trama (capa MAC). Se limita a descifrar las señales para reconvertirlas en bits elementales. Por lo tanto, es incapaz de saber si una trama es válida o no. Sin embargo, un repetidor debe ser capaz de detectar una colisión para poder propagarla por el otro lado.

A pesar de trabajar en el nivel 1, tampoco es capaz de interconectar los cables que funcionan a velocidades diferentes. No es aconsejable utilizar un repetidor en casos de mucho tráfico de red. No es posible utilizar un repetidor si los segmentos utilizan modos de acceso diferentes, ya que los modos de acceso se administran en la capa MAC.

Un concentrador (hub) activo también puede hacer la función de repetidor. Es muy raro encontrar actualmente repetidores que se limiten a esta única función.

b. El puente

Función

Un puente (*bridge*) actúa en la capa Conexión de datos. Permite vincular dos o más soportes físicos diferentes, a condición de que se utilicen en ambos lados los mismos formatos de direcciones MAC.



Puente inalámbrico

Un puente interconecta redes de velocidades diferentes gracias a un funcionamiento de «almacenar y enviar» (*store and forward*). Como contrapartida, puede producirse una saturación de los *buffers* internos, generando una pérdida de tramas. Un puente permite la extensión de una red cuya amplitud máxima se ha alcanzado con repetidores. Las funcionalidades del puente pueden codificarse totalmente en un hardware autónomo.

Acción de filtrado

El puente realiza una acción de filtrado sobre el tráfico que ve pasar. Observando la dirección MAC fuente del paquete que llega, es capaz de saber en qué lugar se encuentra la fuente de emisión (aprendizaje del puente). Algunos puentes son programables, lo que permite efectuar una acción de filtrado en algunos campos del paquete Ethernet. Se pueden utilizar para segmentar una red demasiado cargada.

Además, un puente es capaz de detectar una trama no válida: trama demasiado corta, demasiado larga o que tenga un CRC erróneo.

Aprendizaje

El puente va conociendo poco a poco las direcciones de origen de los dispositivos que originan paquetes y su correspondencia de conexión hacia los puertos (algunos dispositivos, como las impresoras, nunca aparecerán en las tablas de los puentes). A cada dirección de origen se le asocia una duración determinada. Cuando esta duración expira, se suprimen el mapeo de las tablas del puente.

Direccionamiento

En algunos casos, el acceso a las direcciones físicas permite no dejar pasar una trama de la que sabe que el destinatario no está al otro lado.

Por el contrario, cuando el puente no sabe dónde se encuentra el destinatario, deja pasar la trama. Además de transmitir los datos destinados a un único destinatario (*unicast*) si es preciso, el puente deja pasar aquellos destinados a un grupo (multidifusión o *multicast*) o a todos (difusión o *broadcast*).

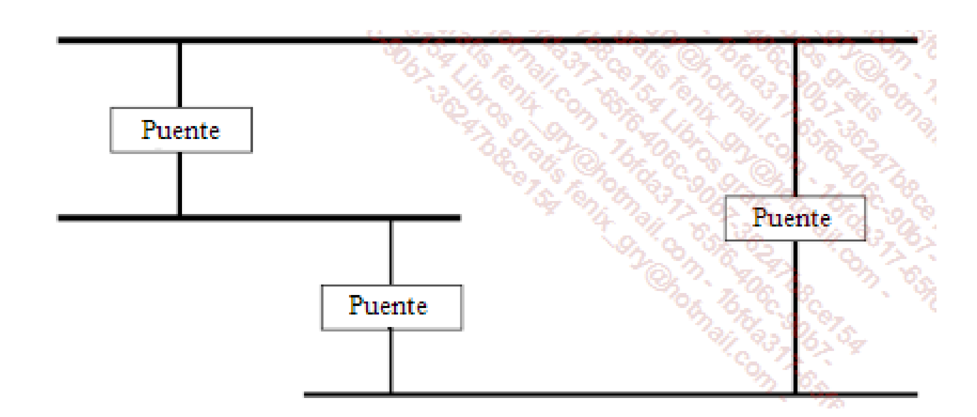
No es necesario asignar direcciones a los puentes, las direcciones de sus interfaces jamás aparecerán en los paquetes, excepto cuando se trata de tramas de servicio intercambiadas entre puentes.

Coherencia del modo de acceso

Al contrario que un repetidor, un puente es capaz de evitar las colisiones sin repetirlas en el otro segmento.

Gracias a sus *buffers*, el puente es capaz de guardar un paquete y de no emitirlo hasta que la red esté dispuesta a recibir la información del otro lado (modo CSMA/CD para Ethernet, o paso de testigo para Token Ring).

Gestión de bucles



Bucle en una red Ethernet

La generalización de las interconexiones de red a través de puentes ha llevado a configuraciones cada vez más complejas. Por ello, los fabricantes han desarrollado un algoritmo de detección de bucle llamado *Spanning Tree Algorithm* (IEEE 802.1D) para Ethernet. En un tipo de configuración bastante particular, si los puentes no detectan el bucle, este genera una circulación continua de tramas que inundan la red. El mismo puente puede detectar el bucle, dirigiendo la trama hacia uno de sus propios puertos mientras está a la escucha de esta trama en otro puerto. En cuanto se detecta el bucle, es necesario desactivar momentáneamente uno de los puertos que participan en el bucle.

 Existe una dirección MAC 01.80.C2.00.00.00, definida para que los puentes puedan dialogar entre ellos.

Interconexión de redes

Basta con utilizar un puente con el fin de desatascar el tráfico (demasiadas colisiones, sobre todo en Ethernet) para tener una red segmentada en dos dominios de colisión diferentes.

Un puente, por definición, solo permite interconectar redes que tengan el mismo método de acceso. Por lo tanto, hablaremos de puentes Ethernet o de puentes Token Ring. Sin embargo,

existen puentes que integran la transmisión de trama y que permiten la interconexión de topologías que administran modos de acceso diferentes. Hay que tener en cuenta que la dificultad reside en la detección de bucle que se realiza en Ethernet gracias a Spanning Tree, mientras que en Token Ring se aplica el algoritmo del origen del enrutamiento.

Los puentes y las métricas asociadas

Los puentes se pueden dividir según dos características:

- **La capacidad de filtrado**: la capacidad de filtrado corresponde al número de paquetes por puerto que un puente puede tratar, para saber si el paquete se debe transmitir.

Por ejemplo, en Ethernet a 10 Mbps, hay que filtrar 14.880 paquetes por segundo, con*buffers* no superiores a 10 KB.

- **La capacidad de transferencia**: la capacidad de transferencia mide el número de paquetes que se pueden transferir en un segundo a otro segmento.

Algoritmo de Spanning Tree

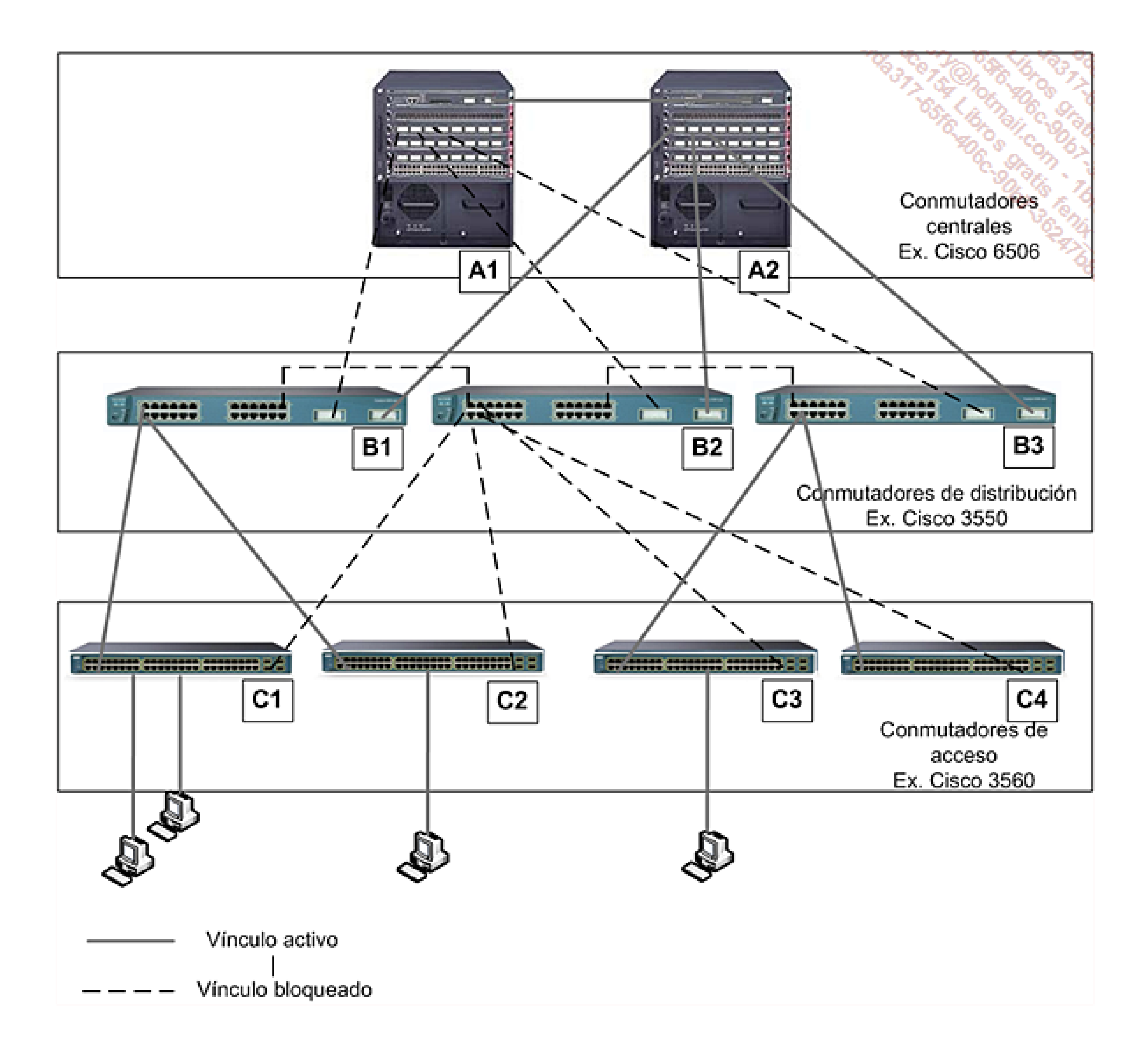
La red se está convirtiendo cada día más indispensable y necesita mecanismos de tolerancia a fallos. La red de nivel 2, al contrario que la de nivel 3, no sabe administrar directamente los múltiples caminos entre un emisor y un receptor. Así, en el caso de los bucles de nivel 2, un conmutador ve que se puede acceder a un ordenador a través de varios de sus puertos (la misma dirección MAC se verá en varios puertos diferentes); en este caso, se generarán tramas duplicadas que pueden llevar al colapso de la red.

El Spanning Tree, literalmente «árbol de expansión», ofrece una solución de neutralización de bucles, que se han introducido voluntariamente en la topología Ethernet para tener mayor tolerancia a fallos.

El algoritmo permite construir, a partir de la topología existente, una arborescencia desde la raíz de un árbol para llegar a cada segmento de la red.

A partir del momento en que el Spanning Tree se ha activado en todos los conmutadores, se opera una neutralización de los bucles calculando el «mejor camino» para el acceso a cada segmento.

En el siguiente esquema, el conmutador central de red A2 ha sido elegido raíz del árbol:

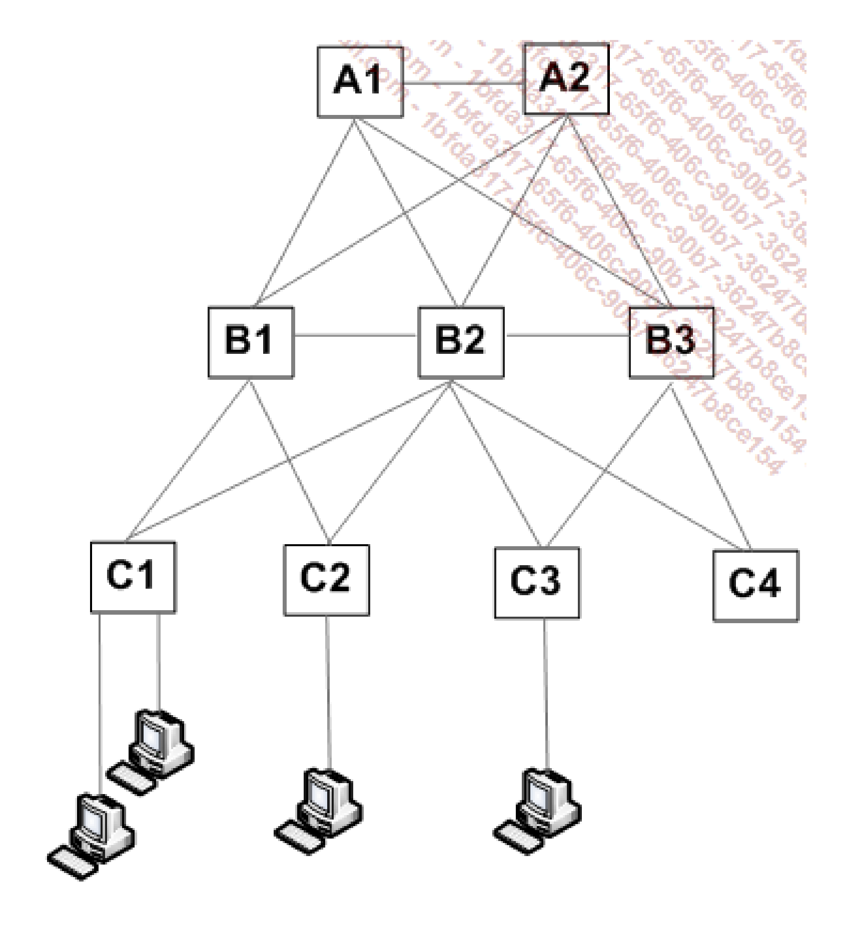


Neutralización de los vínculos por el Spanning Tree.

Observe que, en el esquema, se puede acceder directamente a la red troncal principal a través de los núcleos A1 y A2.

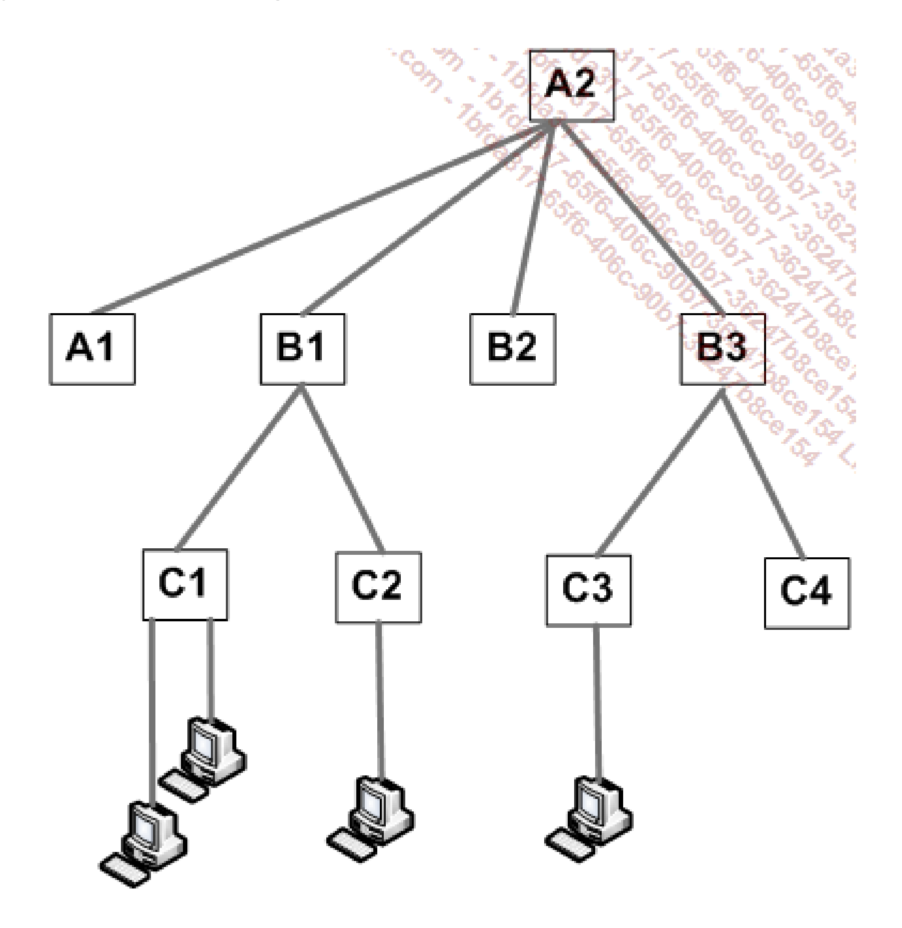
Los servidores de red local están conectados a los servidores de distribución.

Antes de la aplicación de Spanning Tree, el esquema de red era el siguiente:



Esquema de red global

Después de la ejecución de Spanning Tree, el árbol de red equivalente obtenido es el siguiente:



Árbol obtenido por el Spanning Tree

El algoritmo utilizado permite realizar un cierto número de acciones. Para ello se van a intercambiar las tramas entre conmutadores, los mensajes BPDU o Bridge Protocol Data Unit, para obtener la

información en los conmutadores, así como la topología existente.

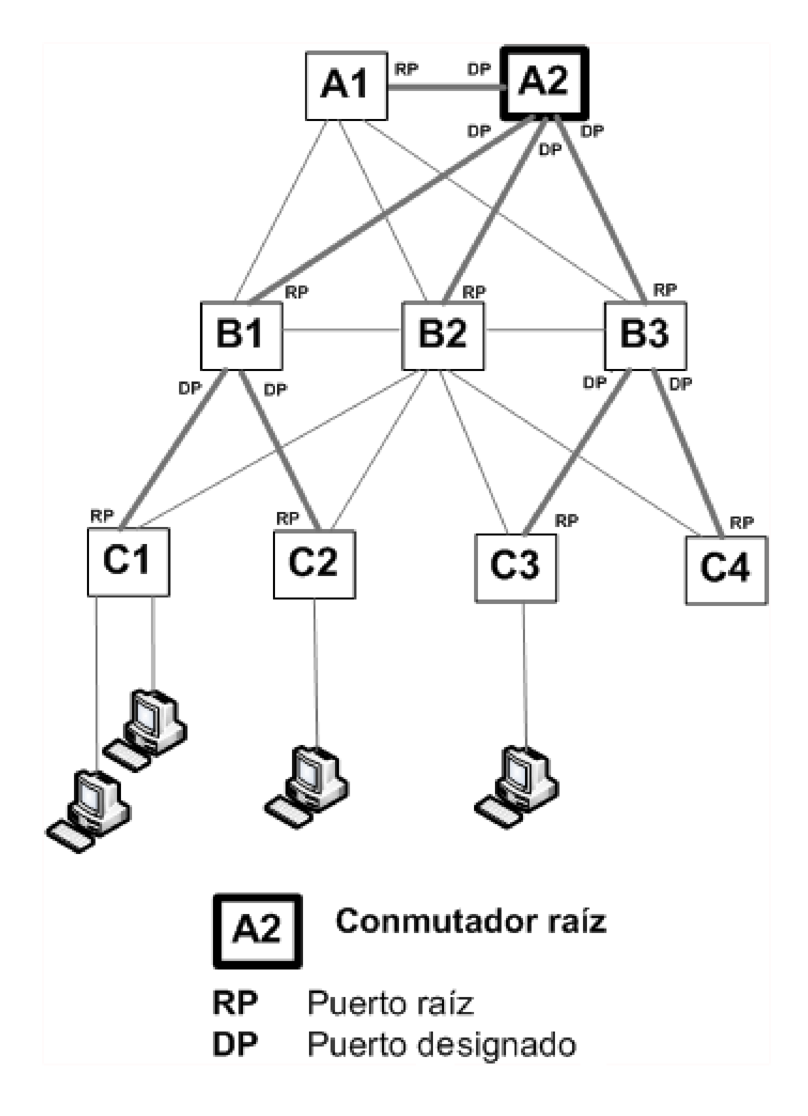
Los objetivos contemplados son los siguientes:

1) Elección de un conmutador raíz del árbol, que disponga de la pareja (prioridad, dirección MAC) más fiable.

2) Designación de otros conmutadores como «conmutadores designados», definiendo un puerto raíz, que necesitará el puerto prioritario para el acceso al conmutador raíz, teniendo en cuenta el camino más corto. Para esto se asociará un coste a cada puerto en función de la velocidad implementada:

Velocidad	Coste
10 Mbps	2.000.000
100 Mbps	200.000
1 Gbps	20.000
10 Gbps	2.000

El «puerto raíz» del conmutador se relacionará entonces con un «puerto designado» de otro conmutador, «acercándose» al conmutador raíz.



Asignación de «puertos raíces» y «puertos designados»

3) Se atribuirán igualmente los puertos complementarios para implementar la redundancia de Spanning Tree (puerto alternativo, puerto de seguridad, etc.).

Así, los puertos en origen de caminos suplementarios se «bloquearán» para impedir el paso de las tramas, pero no el enrutamiento de los mensajes BPDU.

El algoritmo debe ser capaz de reconsiderar la topología de red en cada evolución (corte de red, introducción de un vínculo suplementario, etc.).

c. El conmutador

Origen

El conmutador (*switch*) apareció en 1990 en Ethernet y en 1994 en Token Ring. Integra a la vez la funcionalidad de un *hub* y de un puente. La gestión de este hardware inteligente la realiza un microcontrolador o incluso un microprocesador.

Hoy en día, el conmutador es un componente clave en las redes locales. En todas las redes modernas, los equipos de trabajo y los servidores están conectados directamente a estos equipos. Actualmente es muy raro utilizar concentradores o puentes.

La red ya no tiene una característica de difusión, sino de conmutación.

Los conmutadores se dividen en función de su capacidad de tratamiento respecto del modelo OSI. Los de nivel 2 (N2) o de grupo de trabajo realizan operaciones hasta la capa de datos. Por ejemplo, pueden operar con direcciones MAC de los ordenadores conectados a sus puertos.

Los de nivel 3 (N3), o conmutadores de fase, pueden trabajar con encabezados de capa 3 (Red). También pueden reconocer las direcciones IP.

Por ejemplo, en una utilización típica de estos conmutadores, un núcleo de red de nivel 3 dirige el conjunto de la red. Los servidores pueden estar conectados directamente. Los equipos de trabajo se conectan a los puertos de conmutadores de nivel 2 que utilizan, como administrador, el núcleo de la red.



Conmutadores Ethernet

Principios

El principio de un conmutador Ethernet es posibilitar un segmento a 100 Mbps (incluso 1 Gbps) por puerto y que cada uno esté conectado a un ordenador. Cuando se transporta una trama a partir de un puerto, el commutador establece un circuito virtual (CV) que corresponde a la dirección MAC origen y a la dirección MAC destino para los puertos especificados.

El conmutador es capaz de almacenar una serie de direcciones MAC por puerto (por ejemplo, 1000 entradas por puerto). Las siguientes tramas se conmutan directamente hacia el destinatario correcto, utilizando el CV previamente establecido.

Se trata de una función de puenteo, si bien la conmutación puede hacerse en paralelo en el conjunto de los puertos gracias a la capacidad del conmutador.

Un conmutador puede tener hasta 48 puertos, más dos de interconexión (mediante cable cruzado o fibra óptica).

Tipos de conmutación

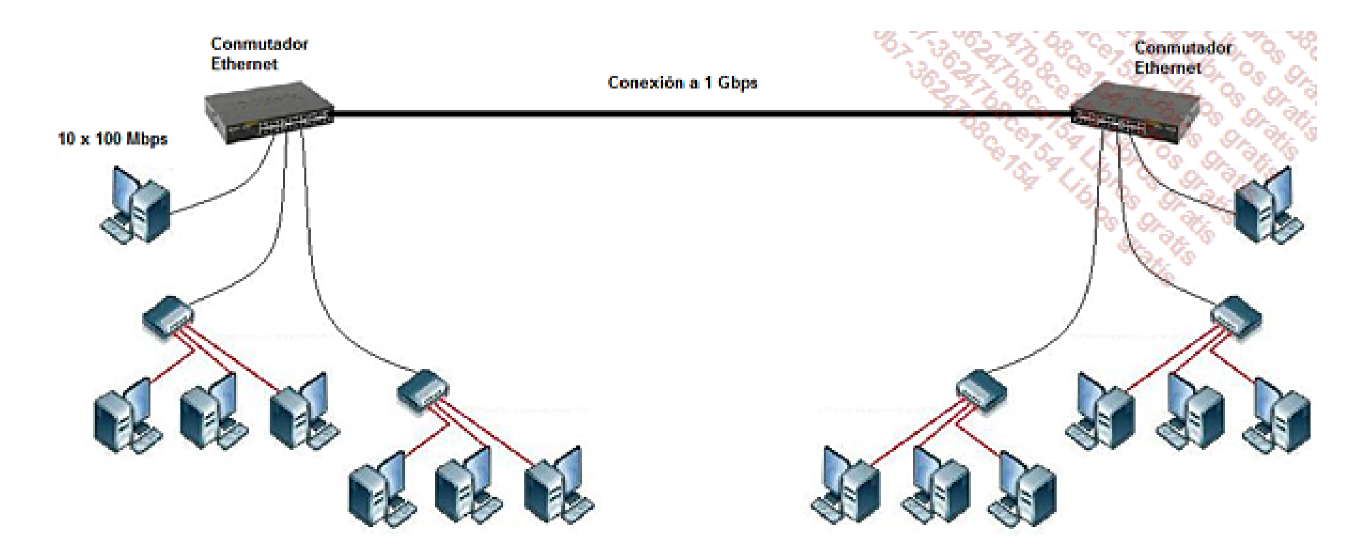
Existen varias clases de conmutación.

La conmutación al vuelo (*on the fly* o *cut through*) responde a un tratamiento simultáneo de tramas, sin almacenamiento intermedio. La ventaja es que el conmutador solo necesita de un pequeño *buffer* y que el tiempo de latencia es inexistente. Sin embargo, deja pasar las tramas erróneas y se transmiten las colisiones.

En la conmutación «almacena y envía» (*store and forward*), se almacena la trama, se analiza y a continuación se encamina hacia el destinatario correcto. Esta técnica tiene la ventaja de eliminar las tramas erróneas.

En Ethernet, el conmutador permite segmentar la red en varios dominios de colisión. En un caso ideal, si se coloca un equipo por puerto, se obtiene una red sin colisión.

La mejora de calidad de los cables cruzados de cobre permite una comunicación a 1 Gbps de bajo coste. Por eso actualmente estas velocidades son normales en las conexiones de red de los servidores y entre conmutadores.

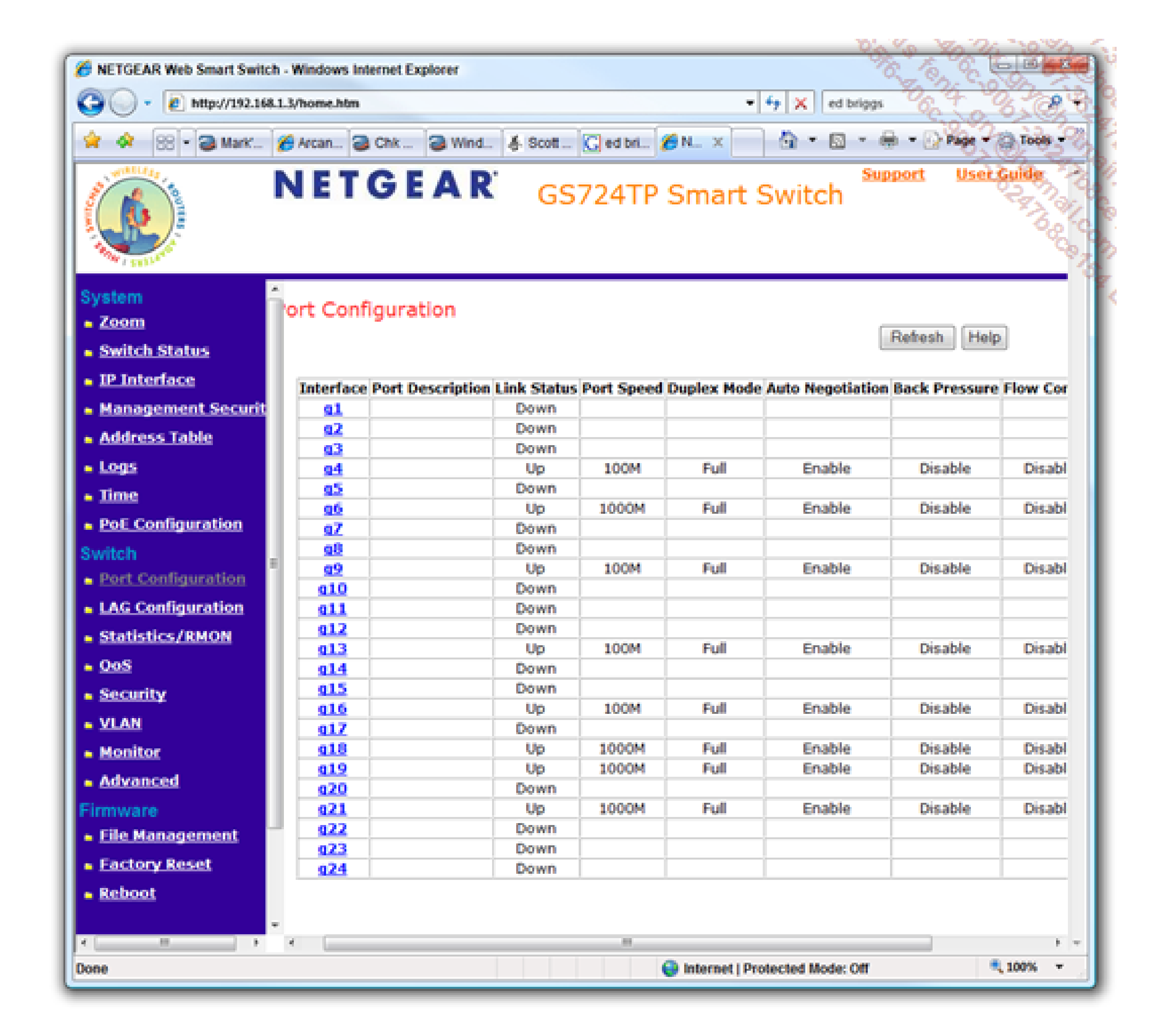


Administración

Muchos conmutadores proporcionan funcionalidades de administración, seguimiento, segmentación de la red y neutralización de bucles (heredada de Spanning Tree, IEEE 802.1D en Ethernet).

En general, disponen de una dirección IP que permite al administrador conectarse a distancia, por Telnet o HTTP, o directamente a través de un terminal serie.

La siguiente pantalla muestra la configuración de los puertos en un conmutador de la marca Netgear.



Administración de un conmutador a través de una interfaz Web

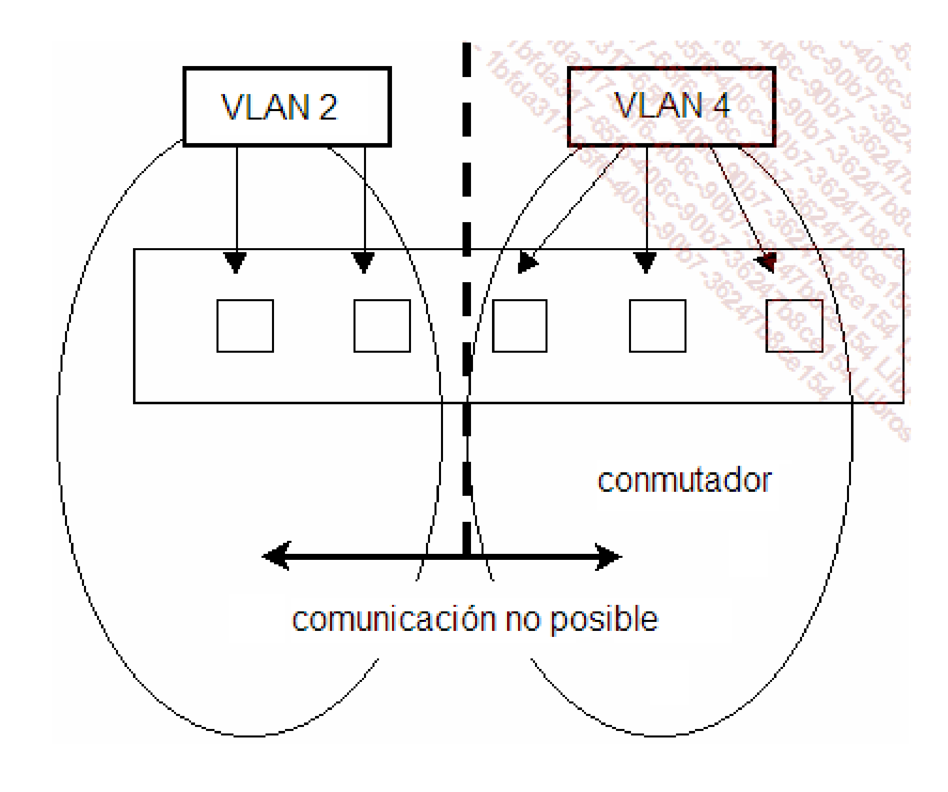
El concepto de VLAN

El objetivo de una red local virtual (VLAN - *Virtual Local Area Network*) es la segmentación lógica de las redes. De este modo, es posible controlar o incluso impedir cualquier diálogo entre equipos interconectados en un mismo conmutador, mediante listas de control de acceso.

La división lógica se puede efectuar de varias maneras. Una VLAN, calificada como implícita, se puede realizar a partir de distintos criterios:

- los números de los puertos del conmutador, capa 1 OSI;
- las direcciones MAC de los dispositivos conectados, capa 2 OSI;
- el protocolo utilizado, capa 3 OSI.

Este último caso se reserva para conmutadores modernos, llamados de nivel 3.



Principio de estanqueidad entre VLAN

Por ejemplo, en una VLAN basada en las direcciones MAC, las que correspondan a una de las VLAN no podrán comunicarse con las que correspondan a otra, salvo si las VLAN están enrutadas.

Un puerto puede pertenecer a varias VLAN.

Tipo de VLAN	Capa OSI	Ventajas	Desventajas
VLAN por puerto	1	• Estanqueidad máxima en caso de intrusión. • Facilidad de configuración por asignación de VLAN en un puerto de un conmutador.	• Configuración pesada a implementar en cada conmutador. • Necesidad de modificar la configuración en cada cambio de puesto. • No hay arquitectura centralizada, cada conmutador dispone de su propia tabla de correspondencia.
Dirección MAC	2	• Posibilidad de centralización de las direcciones MAC para una asignación automática en la VLAN (a través de VMPS o *VLAN Membership Policy Server*).	• Ofrece una seguridad menor que la VLAN por puerto, ya que es posible suplantar una dirección MAC.
Protocolo utilizado	3	• El conmutador asigna automáticamente una máquina a la VLAN en	• Las demoras relacionadas con la desencapsulación de

		función de su dirección IP extrayendo su IP de origen.	las tramas para extraer la dirección IP. • Necesidad de utilizar equipos costosos que aseguren la implementación hasta el nivel 3. • La usurpación de direcciones IP es más fácil de realizar que la usurpación de direcciones MAC.

Existen dos tipos de VLAN: las VLAN implícitas y las VLAN explícitas.

En el funcionamiento de la VLAN implícita, no se modifican las tramas. La pertenencia a una VLAN se basa en el número del puerto, en las direcciones MAC o en un protocolo específico.

En función de esta pertenencia a una VLAN, se rechazará o autorizará la transmisión. Una VLAN implícita sobreentiende una ausencia de marcaje (modificación) de las tramas. Hablaremos entonces de *untagged VLAN*.

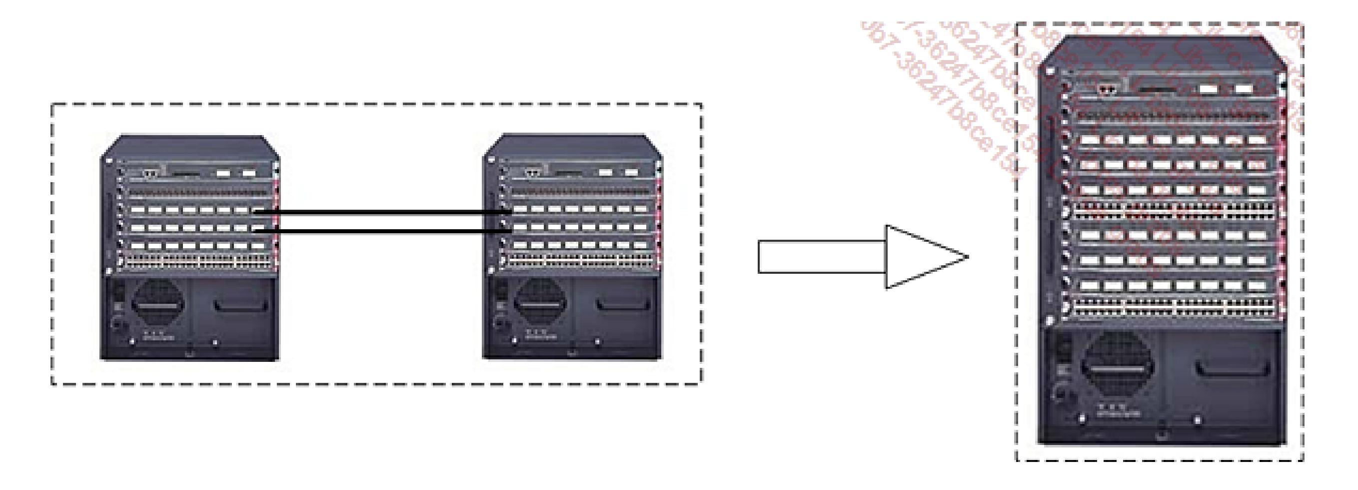
El funcionamiento de VLAN explícita se basa en el marcaje de las tramas (*tagged VLAN*) atendiendo a la norma IEEE 802.1Q.

Este último enfoque permite administrar la segmentación en un entorno de varios conmutadores. Así, se puede rechazar una trama procedente de una *tagged VLAN* de otro conmutador.

Cuando se dispone de varios conmutadores, es posible configurar las conexiones que hay entre los dos dispositivos para optimizar los intercambios. Hablaremos de *Port trunking* para designar la facultad de asociar varias conexiones punto a punto, o de *switch meshing* para designar una malla de conexiones entre un conjunto de conmutadores. Este último enfoque permite poner en práctica una redundancia en conexiones múltiples, designando los mejores caminos entre dos direcciones MAC gracias a distintos criterios, como el tamaño del *buffer*utilizado en cada conmutador y las velocidades asociadas.

Virtualización de conmutadores: VSS

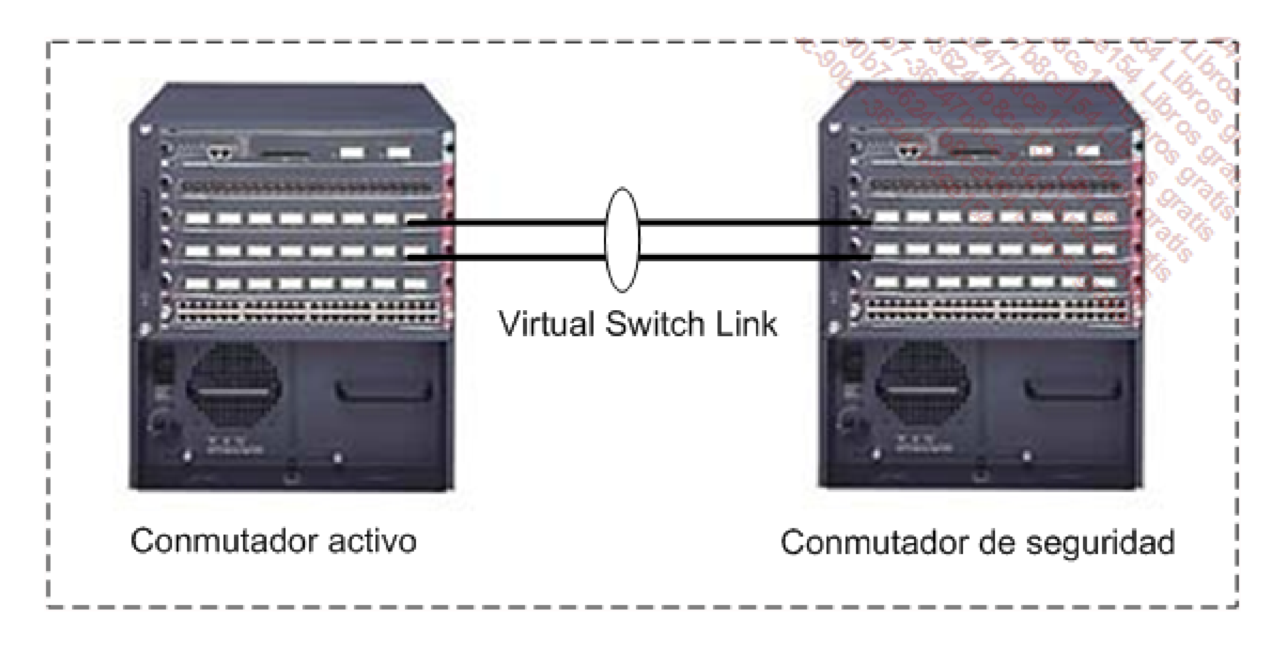
Virtual Switching System (VSS) o sistema de conmutación virtual es una funcionalidad Cisco que permite ver un solo conmutador lógico en lugar de dos conmutadores físicos desplegados (Catalyst 650X). Esta solución permite remplazar con ventajas el Spanning Tree que a menudo aporta complejidad añadida al entorno de nivel 2 existente.



Equivalente lógico a dos Catalyst 650X con VSS

Cada chasis se puede desplegar en una sala técnica distinta, lo que permite ofrecer una solución

con gran tolerancia a fallos.



Conexión de dos conmutadores en VSS

En un sistema VSS, uno de los chasis se designa como conmutador virtual activo y el otro como conmutador virtual secundario. De este modo, solo se elige una de las tarjetas de supervisión como punto de gestión central. De hecho, se puede acceder a las configuraciones de nivel 1, 2 y 3 a través de una configuración única de la tarjeta de supervisión activa.

d. El router

Principio

El router es un dispositivo de interconexión que tiene acceso a toda la información de las capas 1, 2 y 3, en particular, a las direcciones lógicas que son independientes del método de acceso y de la topología física.



El router puede parecer físicamente un conmutador o tener forma de armario:



Conmutador multiniveles

El router modifica la capa física para cambiar el soporte, la capa MAC, para precisar las nuevas

direcciones MAC, la suya y la del próximo periférico intermedio (probablemente otro router), teniendo en cuenta el nuevo modo de acceso. Las direcciones lógicas permiten tener una visión lógica de la intrarred, lo que lleva al router a conocer los distintos caminos posibles para alcanzar un destinatario. El router debe conocer la lista de todas las redes lógicas existentes, que conserva en una tabla. Estos datos se actualizan, ya sea una sola vez al iniciar el dispositivo, lo que llamaremos enrutamiento estático, o bien de manera regular gracias a que los routers se informan entre ellos de las modificaciones de topologías en la intrarred; en este caso se habla de enrutamiento dinámico.

En algunos casos y por razones de seguridad, todas las tablas de enrutamiento pueden ser predefinidas y fijadas.

Una tabla de enrutamiento contiene el conjunto de las direcciones de red conocidas, la manera de conectarse a las otras redes (la dirección lógica del próximo dispositivo que permite llegar a la red del destinatario en el que se encuentra el servidor), los distintos caminos entre routers y los costes vinculados al envío de los datos. Un router también puede hacer la función de barrera de seguridad (cortafuegos) filtrando algunas direcciones lógicas.

El concepto de enrutamiento solo es posible a condición de que los protocolos utilizados sean enrutables, es decir, que administren una dirección lógica compuesta por un número de red y un número de servidor en la red.

Un router, por definición, no deja pasar una difusión (número de redes diferentes).

Un router se puede configurar con un terminal conectado a un puerto DB25 del router, o a través de la red, por ejemplo mediante TELNET en TCP/IP.

Exploración de las rutas

Existen algoritmos de camino único y algoritmos de caminos múltiples que posibilitan una distribución de la carga.

Además, se distingue entre los algoritmos de dominio de enrutamiento plano y los de dominio jerárquico, que evitan que los routers tengan que aprender todas las redes lógicas posibles.

En todos los casos, un router debe elegir el mejor camino posible según distintos criterios. El número de saltos (*hops*) corresponde al número de desvíos para cambiar de red, es decir, el número de routers por los que se debe pasar. El TICKS da cuenta del tiempo de travesía necesario en la red. El coste de la línea, la densidad del tráfico, la velocidad de las líneas recorridas, así como su fiabilidad, son otros criterios para poder elegir el mejor camino.

Tipos de routers

Estáticos

En este caso, el administrador inicializa manualmente la tabla de enrutamiento (por ejemplo mediante telnet). Los caminos posibles están predefinidos y los routers intermedios no toman ninguna decisión de enrutamiento.

Dinámicos

A menudo, se configura la primera ruta manualmente y se escoge el mejor camino al pasar por cada router de la red.

Elección de una distancia

Vector de distancia

Cada router construye su propia tabla de enrutamiento, en la que combina la información de las tablas de sus vecinos inmediatos.

El inconveniente reside en el hecho de que este tipo de algoritmo genera mucho tráfico en la red. Las tablas de enrutamiento completas se difunden por defecto cada 30 segundos. Además, requiere un tiempo de convergencia bastante largo.

Ejemplo:

IP e IPX aceptan *Routing Internet Protocol* (RIP).

Estados de conexión

La exploración de las rutas se basa en una difusión global inicial, a continuación se difunde cada modificación por separado. Así, las tablas de enrutamiento están permanentemente al día.

Ejemplos:

Open Shortest Path First (OSPF) es utilizado por IP (trabaja a nivel jerárquico).

Podemos citar igualmente los protocolos de enrutamiento IGRP (*Interior Gateway Routing Protocol*) y EIGRP (*Enhanced IGRP*), desarrollados por CISCO. Muy fiables y extensibles, solucionan las limitaciones de RIP.

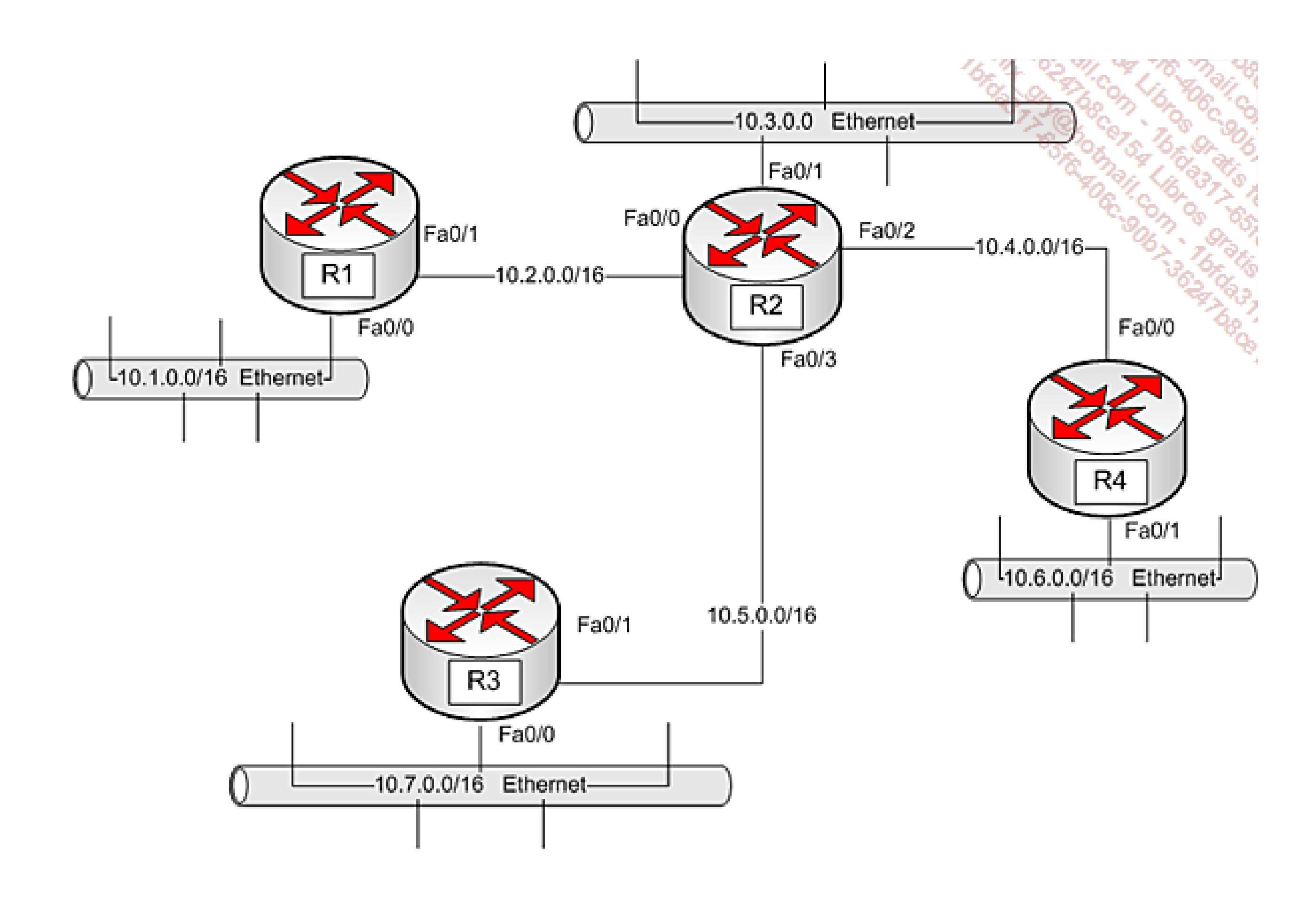
Ejemplo de protocolos de enrutamiento

RIP

El protocolo RIP (*Routing Information Protocol*), inicialmente especificado en la RFC 1058 (RIPv1) y posteriormente en la RFC 2453 (RIPv2), es un protocolo de enrutamiento interno y utiliza un algoritmo de vector de distancias.

Utiliza el número de saltos como medida para la selección del camino. Establece como ruta inaccesible un número de saltos superior a 15. Cada router RIP envía el contenido de su tabla de enrutamiento, por defecto cada 30 segundos, a sus vecinos.

Cuando un router recibe una actualización que incluye una nueva subred o una modificación, el router actualiza su tabla de enrutamiento. A nivel de cada router, el valor del número de saltos se incrementa en una unidad. Después de haber actualizado su tabla de enrutamiento, el router comienza a transmitir las actualizaciones de enrutamiento para informar a los demás routers de la red. El envío de estas actualizaciones, llamadas actualizaciones desencadenadas, es independiente del envío de actualizaciones regulares por los routers RIP.



Entorno de red y RIP

Inicialmente, los routers conocen las redes a las que están conectados. Lo que da:

Router R1	Red	Interfaz	Salto
	10.1.0.0/16	Fa0/0	0
	10.2.0.0/16	Fa0/1	0

Router R2	Red	Interfaz	Salto
	10.2.0.0/16	Fa0/0	0
	10.3.0.0/16	Fa0/1	0
	10.4.0.0/16	Fa0/2	0
	10.5.0.0/16	Fa0/3	0

Router R3	Red	Interfaz	Salto
	10.7.0.0/16	Fa0/0	0
	10.5.0.0/16	Fa0/1	0

Router R4	Red	Interfaz	Salto
	10.4.0.0/16	Fa0/0	0
	10.6.0.0/16	Fa0/1	0

Cuando R1 difunda su tabla de enrutamiento a su vecino R2, R2 descubrirá la existencia de la red 10.1.0.0/16 por su interfaz Fa0/0:

Router R2	Red	Interfaz	Salto

	10.2.0.0/16	Fa0/0	0
	10.3.0.0/16	Fa0/1	0
	10.4.0.0/16	Fa0/2	0

Capas bajas e IEEE

Numerosos protocolos concretan las capas bajas del modelo OSI, es decir, la capa física y de Conexión de datos, que siguen siendo independientes de las capas superiores.

Distintos organismos, como el *Institute of Electrical and Electronic Engineers* (IEEE) han estandarizado estas tecnologías.

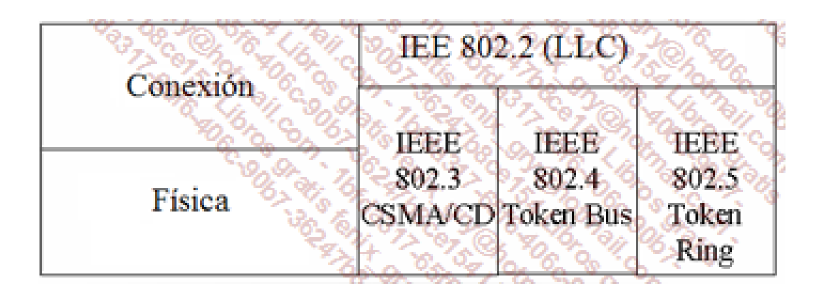
1. Diferenciación de las capas

La capa física se asocia a la interfaz mediante cable o de forma inalámbrica. Se definen distintas características, como el método de acceso al soporte, la codificación, las topologías soportadas, la velocidad...



La tarjeta de red

El proyecto 802 del IEEE divide el nivel conexión de datos en dos capas inferiores. La primera se llama control de acceso a los medios de comunicación o *Medium Access Control* (MAC) y es inherente a cada tipo de red. La segunda se llama control de la conexión lógica o *Logical Link Control* (LLC), es independiente del tipo de red y está estandarizada como 802.2.



Conexión	IEE 802.2 (LLC)		
Física	IEEE 802.3 CSMA/CD	IEEE 802.4 Token Bus	IEEE 802.5 Token Ring

Las normas 802.x del IEEE

2. IEEE 802.1

Esta especificación es una introducción a las normas 802 e implica las relaciones globales entre todas las otras especificaciones. Tiene en cuenta los problemas relativos a la gestión de los sistemas y a la interconexión de redes.

Por ejemplo, el algoritmo de *spanning tree*, que soluciona los problemas de bucles en las redes Ethernet, se describe en 802.1D. El marcado en las VLAN explícitas se define en 802.1Q. La gestión de las prioridades se aborda en 802.1P.

3. IEEE 802.2

a. Principios de Logical Link Control (LLC)

El control de capa de conexión define servicios estándar, cualquiera que sea la topología y el método de acceso al soporte. Controlan conexiones punto a punto o multipunto en soportes limitados o ilimitados, en *half-duplex* o en *full-duplex*, en redes de conmutación de paquetes o de circuitos.

LLC puede garantizar la integridad de la transmisión de extremo a extremo entre dos estaciones.

High level Data Link Control (HDLC) es un protocolo creado en 1979 que corresponde a una etapa intermedia de LLC.

b. Tipos de servicio

Los protocolos LLC ofrecen tres tipos de servicio.

Servicio sin conexión ni confirmación (tipo 1)

Es el servicio más simple y menos fiable. Es también el más utilizado, ya que a menudo la mayoría de los protocolos utilizan un transporte seguro (capa 4 OSI).

Servicio orientado a la conexión (tipo 2)

Consta de una conexión lógica entre el emisor y el receptor.

Servicio sin conexión con confirmación (tipo 3)

Cada trama se confirma individualmente, pero no existe conexión lógica entre las dos estaciones.

Ethernet e IEEE 802.3

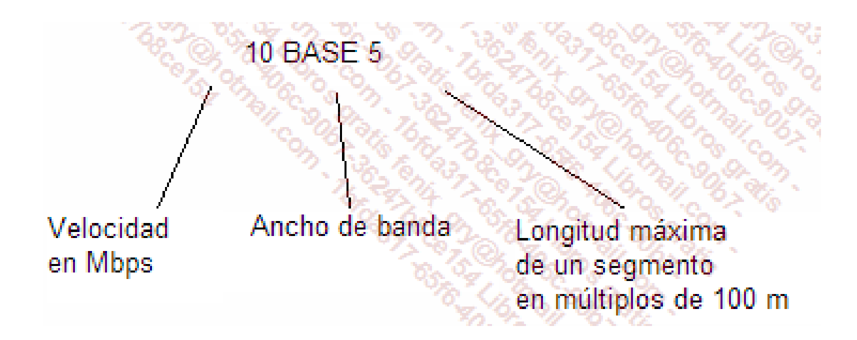
1. Generalidades

El protocolo Ethernet aparece en 1980 como resultado de los trabajos de DEC, Intel y Xerox. Como es tan económico, está siempre presente en cualquier instalación. Su evolución se estandarizó en la norma IEEE 802.3, que cubre la capa Física y una parte de la de Conexión de datos. Hay algunas diferencias entre Ethernet y 802.3, pero no disociaremos estas dos normas.

802.3 utiliza los servicios de la capa LLC. El modo de acceso al soporte es por contención, a través de *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD).

2. Características de la capa Física

802.3 ofrece distintas opciones de capa Física. Las denominaciones utilizadas toman en cuenta la velocidad, el soporte, el tipo de señal y la longitud del segmento.



10 base 2 corresponde a una red Ethernet con cable coaxial fino (10 Mbps, señalización digital para segmentos de 200 metros como máximo; en realidad, 185 metros).

10 base T corresponde a una Ethernet con par trenzado (T por *Twisted pair*).

100 base T es una implementación de Ethernet a 100 Mbps con par trenzado (categoría 5).

1000 base T (norma IEEE 802.3ab) corresponde a una solución basada en el par trenzado UTP categoría 5e (máximo 100 metros).

10 G base T se basa en la definición IEEE 802.3an y establece la velocidad a 10 Gbps para el par trenzado en longitudes máximas de 100 metros.

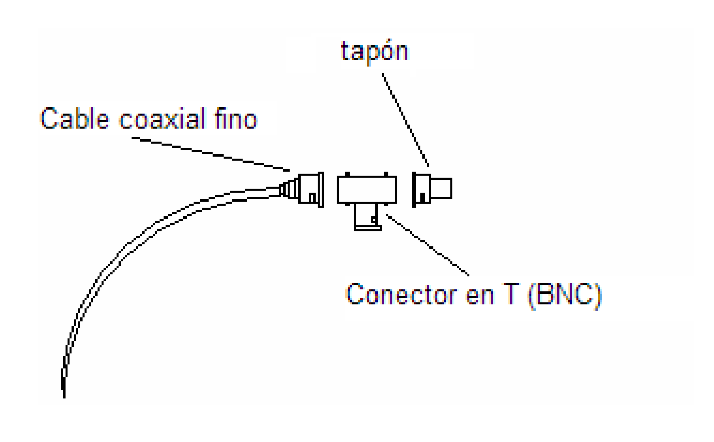
La señalización es digital y la codificación utilizada es la Manchester (las tarjetas de red funcionan a 20 MHz). Una trama tiene una longitud mínima de 64 bytes y máxima de 1518 bytes.

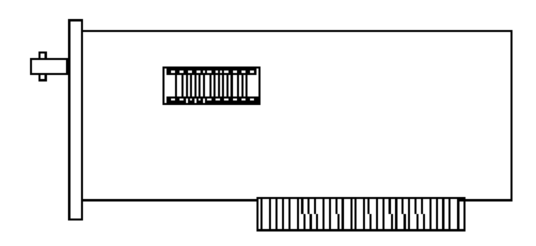
a. Las especificidades de Ethernet

Ethernet se definió para una velocidad de 10 Mbps. En un principio se conectaban los nodos de la red con cable coaxial grueso (*thick*) o fino (*thin*). Más tarde, la casi totalidad de las implementaciones de este tipo de red utilizan el par trenzado o incluso la fibra óptica.

10 base 2

Una red Ethernet que utiliza el coaxial fino RG58, de 5 mm de diámetro, se llama *thin-net* o*cheap-net*.



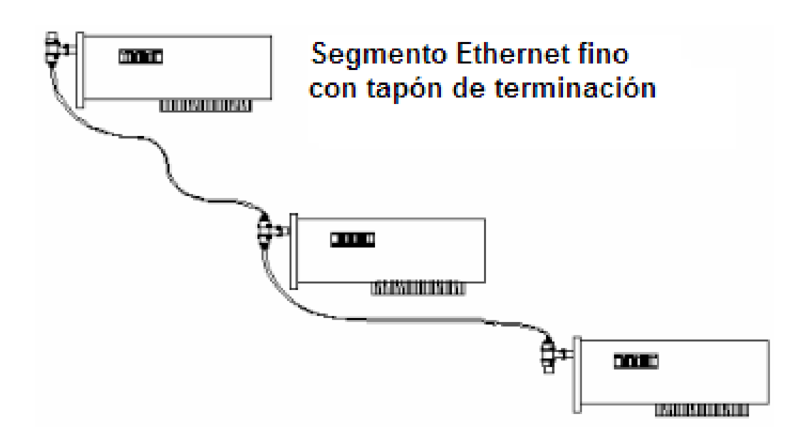


La topología preferida es el bus y los segmentos no deben exceder los 185 metros (debido al importante factor de atenuación). Utilizaremos conectores *British Naval Connector* (BNC) para conectar los nodos.



Conector en «T»

La distancia mínima entre dos conectores T es de 0,5 m. El número máximo de estaciones es de 30 por segmento. El alcance de la red no debe superar los 925 metros (interconectando como máximo 5 segmentos con 4 repetidores). Es necesario colocar una resistencia o tapón de terminación en cada extremo del segmento. El transmisor-receptor que permite la circulación de las señales está integrado en la tarjeta de red de 10 base 2.



10 base 5

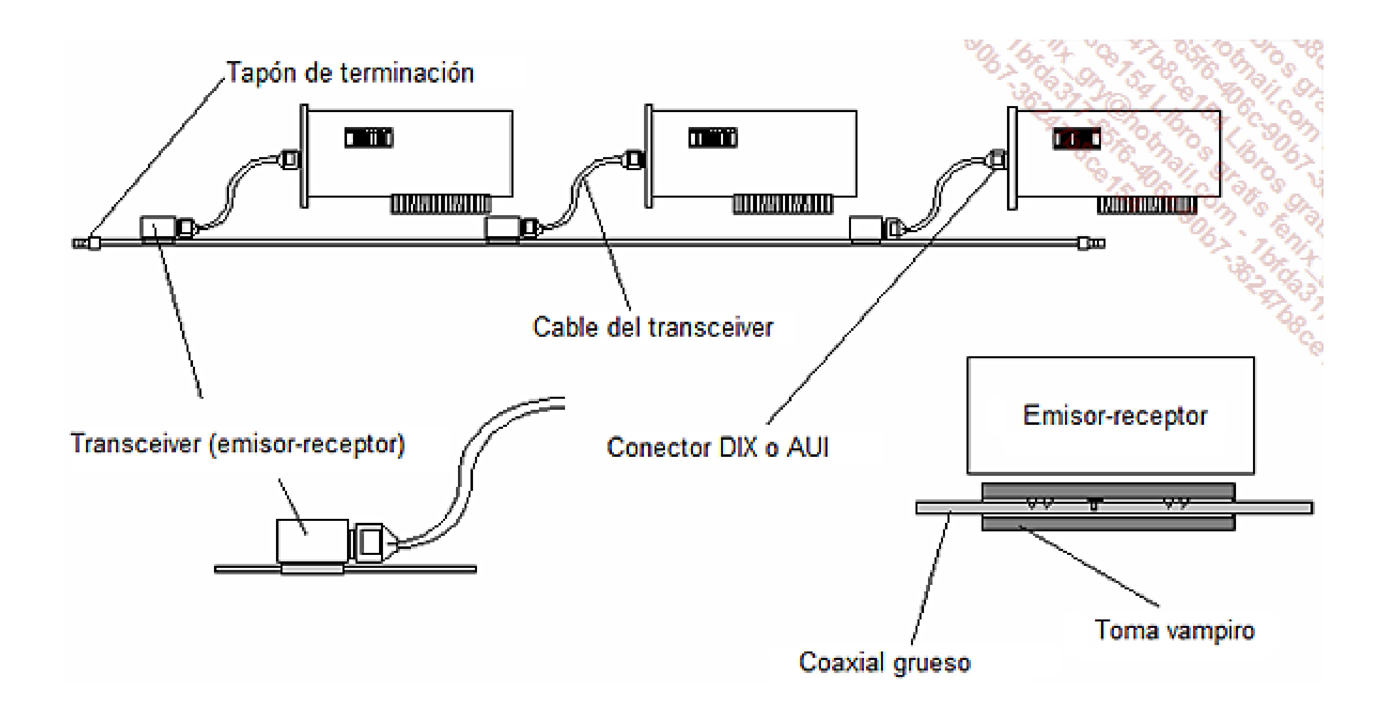
El soporte coaxial grueso RG11, de 10 mm de diámetro, casi ha desaparecido, aunque todavía se utiliza en entornos muy sensibles a las interferencias electromagnéticas.



Cable coaxial grueso

Las redes Ethernet que utilizan el cable coaxial grueso también se conocen con los nombres*thick-net*, gran Ethernet o Ethernet gruesa, en función de su volumen y de su rigidez. El modo de acceso CSMA/CD funciona como en 10 base 2, en una topología de bus. Los segmentos llegan a los 500 metros, lo que confiere a la red un alcance máximo de 2500 metros.

En Ethernet, se habla a menudo de la regla 5-4-3, que permite tener como máximo 5 segmentos interconectados por 4 repetidores. De los 5 segmentos, solo 3 deben estar conectados a equipos de trabajo. Así, en la Ethernet fina, el alcance máximo de la red es de 925 metros contra 2500 en la Ethernet gruesa.



En el caso del 10 base 5, el emisor-receptor (o *transceiver*) es externo y puede alejarse de la tarjeta de red a unos 50 metros. El cable que conecta el *Access Unit Interface* (AUI) o *Digital Intel Xerox* (DIX) de la tarjeta con el *transceiver* a través del cable coaxial grueso se llama cable emisor-receptor. La distancia mínima entre dos *transceivers* es de 2,5 metros y no se deben tener más de 100 *transceivers* por segmento.

El emisor-receptor externo a menudo se conecta al cable grueso utilizando una toma vampiro. También encontramos adaptadores AUI/RJ45, que disponen de un emisor-receptor integrado que permite conectar la tarjeta de red 10 base T utilizando un conector AUI.

10 base T

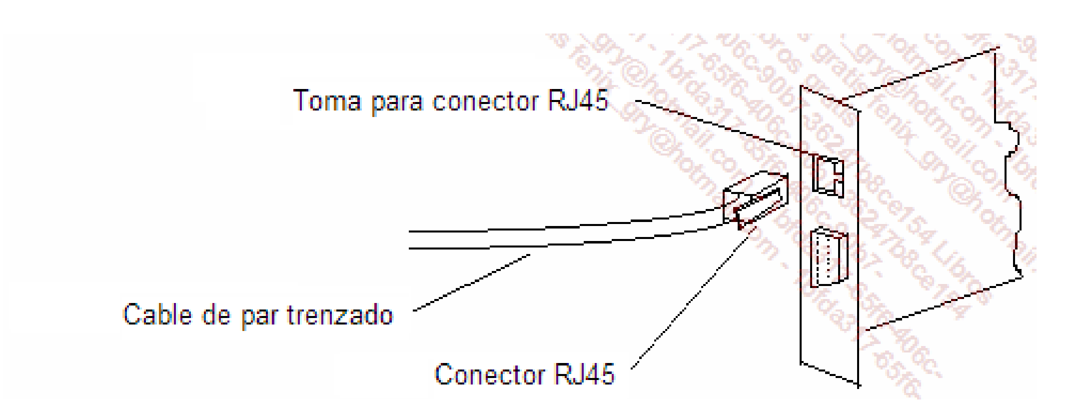
Las redes Ethernet en estrella utilizan el cable de cobre de par trenzado. Se emplean cuatro hilos, acoplados a conectores RJ45. El cable utilizado es de categoría 3 o 5 y puede estar blindado o no.



Cable 10 base T

La red se forma por centralización en un conmutador (*switch*). La longitud del cable entre el hardware que se desea conectar y el elemento activo no debería, teóricamente, exceder los 100 m. Con la mejora de calidad de los cables esta distancia se puede superar en la práctica, aunque no se recomienda.

Aunque la imagen externa, proporcionada por la conexión entre los distintos puertos del elemento activo, se parece a una estrella, los nodos de la red componen una topología en bus. Se puede ampliar la red conectando los elementos activos en cascada, para obtener una topología en árbol, o interconectándolos mediante un bus (con frecuencia de fibra óptica).



Ethernet y la fibra óptica

Fiber Optic Inter Repeater Link (FOIRL) fue la primera implementación de la fibra óptica en una red Ethernet.

La fibra óptica se puede utilizar para la conexión de dos LAN situadas a distancias relativamente cercanas (uno o dos kilómetros).

La interconexión puede efectuarse por medio de un repetidor, de un puente o incluso de una estrella óptica activa (gestión de colisiones).

Siempre hay que utilizar dos fibras, que son soportes simplex, para asegurar la emisión y la recepción.

La utilización de la fibra a bajas velocidades ha permitido crear soluciones para Ethernet, con longitudes de segmentos que llegan hasta los dos kilómetros. Una posibilidad es utilizar la fibra para interconectar LAN distantes con ayuda de repetidores mixtos (fibra/coaxial, por ejemplo).

A finales de 1993, se definieron algunos estándares para Ethernet y la fibra óptica. Se les designa con el nombre 10 base F. Estas especificaciones definen tres tipos de segmentos: 10 base FL (*Fiber Link*), 10 base FB (*Fiber Backbone*) y 10 base FP (*Fiber Passive*).

10 base FL

Esta norma, que sustituye al antiguo FOIRL, define un segmento de punto a punto que puede

alcanzar los 2 km, a condición de que solo se utilicen equipos 10 base FL. Si se utiliza algún equipo FOIRL, el segmento no llegará a más de 1 km. Un segmento 10 base FL puede unir dos ordenadores o dos repetidores, o un ordenador a un puerto de un repetidor.



Repetidor 10 base FL

10 base FB

Esta especificación permite definir una topología basada en fibra óptica, como troncal de una arquitectura de estrella. Esta implementación describe una indicación sincrónica que permite ir más allá del número de repetidores aceptados por Ethernet. Las conexiones 10 base FB no conectan ordenadores; se utilizan solamente para conectar estrellas ópticas 10 base FB para construir una columna troncal. Cada segmento puede alcanzar los 2 km. Además, esta última norma permite el diagnóstico a distancia de los fallos.



Cable 10 base FB

10 base FP

Este conjunto de especificaciones define una estrella pasiva que enlaza varios ordenadores conectados a una fibra óptica sin utilizar repetidor. Un segmento 10 base FP no debe superar 500 m. Una estrella pasiva 10 base FP puede conectar hasta 33 ordenadores.

Cada vez es menos frecuente encontrar en uso redes Ethernet a 10 Mbps. La mayoría de las implementaciones presentadas con anterioridad ya no se utilizan en absoluto. Sin embargo, sí representan bases en torno a las cuales se han desarrollado técnicas más recientes, como Fast Ethernet.

b. Las especificidades de Fast Ethernet

Con el aumento del tráfico de red necesario en las empresas, la velocidad nativa de 10 Mbps de Ethernet ya no es suficiente. En 1994 apareció Fast Ethernet, su sucesor (estándar IEEE 802.3u), que ofrece un ancho de banda 10 veces superior sin ser más caro.

Durante sus primeras aplicaciones concretas, Fast Ethernet, con su implementación de 10/100 Mbps, permitió tener en cuenta lo que ya existía. Esta capacidad de transición facilitó su puesta en marcha inicial.

El cableado utilizado es el par trenzado de cobre de categoría 5 como mínimo, con conector RJ45, o de fibra óptica.

Fast Ehernet utiliza, igual que su predecesor, CSMA/CD. Las topologías son las mismas.

100 base T4

100 base T4 utiliza cuatro pares trenzados UTP de categoría 3 como mínimo. Los conectores son compatibles con 10 base T y 100 base T4, para el cual utiliza dos pares suplementarios. La codificación es de tipo 8B/6T y utiliza tres de los cuatro pares para transmitir en cada sentido, y el cuarto par para la detección de colisiones.

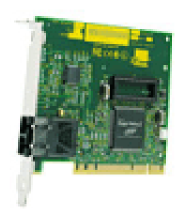
Esta solución permitía inicialmente recuperar arquitecturas basadas en cables de categoría 3. Estos ya no se utilizan y el 100 base T4 ya no resulta interesante.

100 base TX

Esta implementación utiliza par trenzado de categoría 5 como mínimo, blindado o no. La inserción de los cables en los conectores RJ45 es compatible con 10 base T. Se trata del estándar utilizado normalmente.

100 base FX

100 base FX se basa en la fibra óptica (dos fibras).



Tarjeta de red para fibra óptica

Fast Ethernet se ha impuesto como el estándar desde hace ya algunos años. Las velocidades de las estaciones de trabajo parecen suficientes y la aplicación de 100 base TX tiene un coste escaso.

c. Gigabit Ethernet

Esta evolución la estandarizó IEEE con el número 802.3z. La banda ancha más rápida, de 1 Gbps, obliga a revisar las bases de la comunicación. Por ejemplo, los cables de categoría 5 normalmente no se han diseñado para conseguir frecuencias tan rápidas como las necesarias en este caso. La denominación 5e (*enhanced*) designa cables capaces de soportar frecuencias de 100 MHz.

Se asegura la compatibilidad con sus predecesores, de donde procede el calificativo para el hardware: 10/100/1000 Mbps.

Para migrar una instalación existente a gigabit Ethernet, normalmente es necesario hacer un reciclaje. A menudo, aunque el hardware sea adecuado, el cableado no puede soportar la velocidad de una manera fiable.

A 1 Gbps, la gestión de las colisiones es muy delicada. A esta velocidad, las arquitecturas son conmutadas.

Se reconoce un cierto número de implementaciones, como:

- 1000 base T (o 1000 base TX): comparable a 100 base T, pero 10 veces más rápida, admite el par de cobre trenzado de categoría 5 (o mejor de 5e) y 6 en cables con un máximo de

100 metros.

- 1000 base SX (*Short Wave*): para la explotación de fibras ópticas multimodo en distancias más cortas, del orden de 550 metros como mínimo.
- 1000 base LX (*Long Wave*): utiliza la fibra óptica multimodo o monomodo para un máximo de 2 a 5 kilómetros.

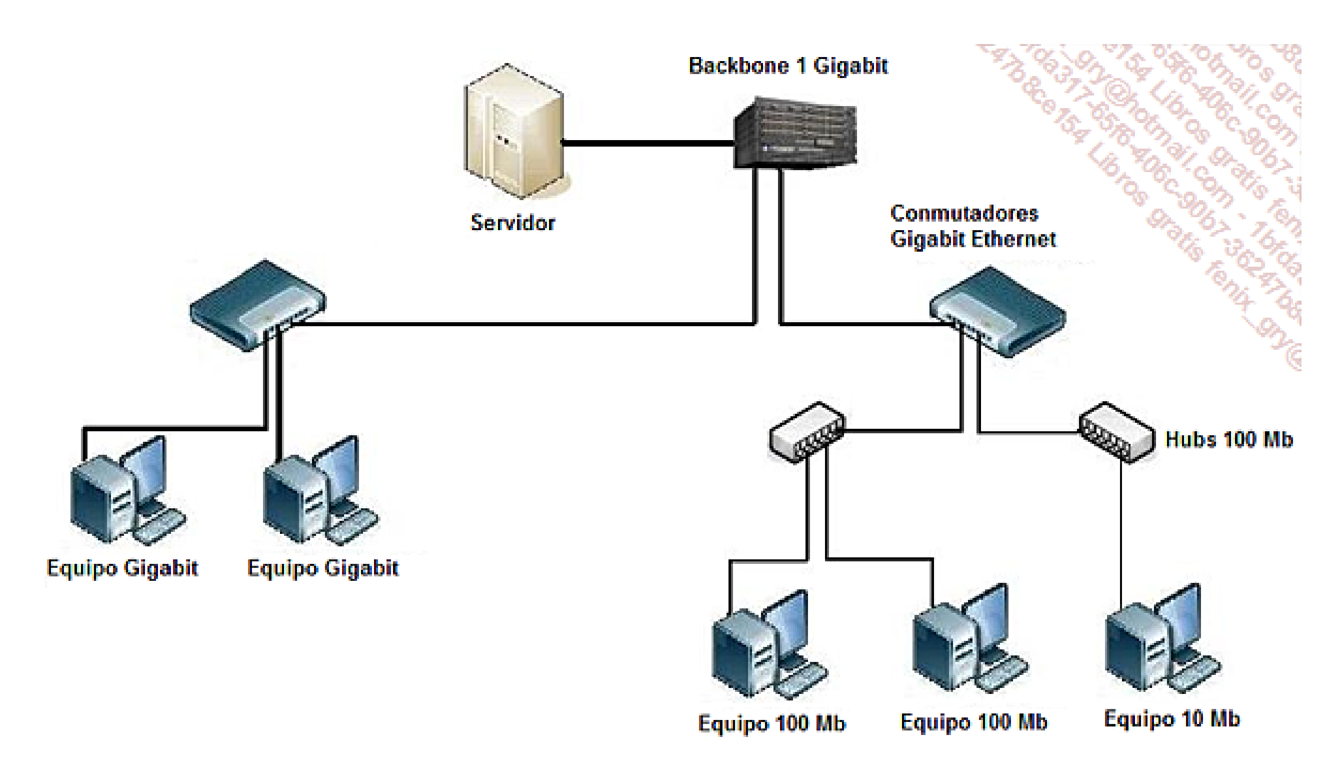


Conmutador compatible con varios conectores de fibra a través de GBIC

Gigabit Ethernet está destinado a enlaces troncales y a las comunicaciones con los servidores.

En el primer caso, permite la interconexión entre conmutadores (fibra óptica o cobre) o bien entre subrepetidores. Si estos dispositivos, que son los que tienen el hardware de conmutación, están alejados o en edificios diferentes, es necesaria una conexión de fibra óptica.

En el caso de los servidores, esta solución es interesante porque generalmente estos forman un cuello de botella y porque las velocidades de red que les corresponden deben ser más elevadas.



Arquitectura Ethernet a diferentes niveles que implementa velocidades variables

Hay una norma complementaria, 802.3x, que define la adaptación de la velocidad con las redes menos rápidas. Como los *buffers* de entrada/salida no son limitados y, por lo tanto, no pueden absorber las diferencias de velocidad, se activa un control de flujo que indica al emisor cuándo tiene que hacer una pausa en la transmisión.

Gigabit Ethernet ya no tiene nada de excepcional en las arquitecturas de red de empresa. Cada vez más interfaces para estaciones de trabajo y ordenadores portátiles pueden alcanzar estas velocidades.

d. 10 Gigabit Ethernet

En el año 2002, IEEE aprobó el 10 Gigabit Ethernet como 802.3ae, sucesor del 802.3z. Sigue siendo compatible con sus predecesores, pero ya no se limita a las redes locales, sino que también se utiliza a nivel metropolitano y de redes extensas.

El objetivo es continuar utilizando el mismo formato de tramas que en la disposición Ethernet original. En contraposición, es indispensable la comunicación de tipo *full-duplex*.

Se han definido siete especificaciones:

- 10 GBASE-CX4 (802.3 ak) utiliza un cable de cobre especial en una distancia máxima de 15 metros.
- 10 GBASE-T (802.3an) con un cable de cobre de categoría 6 (200 MHz), 6a (500 MHz) y 7 (600 MHz), que asegura distancias de comunicación inferiores a 100 metros.
- 10 GBASE-SR (*Short Range*) tiene un alcance de 26 a 82 metros con fibra óptica multimodo (pero puede alcanzar 300 metros con una nueva generación de fibra).
- 10 GBASE-LX4 trabaja con multiplexado por división de longitud de onda y aumenta las distancias soportadas a 240 o incluso 300 metros, con la fibra óptica multimodo (soporta 10 kilómetros con una fibra monomodo).
- 10 GBASE-LR (*Low Range*) utiliza fibra óptica monomodo para comunicaciones de hasta 10 kilómetros.
- 10 GBASE-ER (*Extended Range*) permite distancias de 40 kilómetros, siempre con fibra monomodo.
- 10 GBASE-LRM (*Long Range Multimode*, 802.3aq), permite implementar FDDI en distancias de hasta 200 metros.

Varios fabricantes de hardware han hecho evolucionar el 10 GBASE-ER en 10 GBASE-ZR para ampliar la distancia hasta a 80 kilómetros.

e. 100 Gigabit Ethernet

La norma IEEE 802.3ba se publicó en junio de 2010.

Define velocidades que van de 40 a 100 Gbps para soportes de tipo de fibra óptica o par trenzado.

Existen soluciones basadas en la utilización del cobre para distancias limitadas a 10 metros:

- 40 GBase-CR4
- 100 GBase-CR10

Otras soluciones se basan en la fibra multimodo, pero no permiten más que distancias limitadas (100 a 125 metros):

- 40 GBase-SR4
- 100 GBase-SR10

Las que se basan en la fibra monomodo, permiten llegar a los 10 kilómetros con 40 GBase-LR4 y a los 40 kilómetros con 100 GBase-ER4.

Reciente y bastante costosa, Ethernet a 10 Gbps todavía no está muy implantada en las redes locales, donde una velocidad 10 veces inferior es suficiente.

f. Recapitulación

A continuación exponemos un cuadro recopilatorio con las aplicaciones más frecuentes de las

redes locales.

Denominación	Soporte	Longitud máxima del segmento	Velocidad	Topología
100 Base TX	UTP Cat 5 como mínimo	100 metros	100 Mbps	Estrella (conmutador)
1000 Base TX	UTP Cat 5e como mínimo	100 metros	1 Gbps	Estrella (conmutador)
1000 Base SX	Fibra multimodo doble 62.5/125 µm	550 metros	1 Gbps	Estrella o bus/punto a punto
1000 Base LX	Soporta ondas láser en fibra óptica multimodo y monomodo	5 km	1 Gbps	Subsistemas de campo



Mini GBIC 100 Base SX Gigabit LC

3. Encabezados de trama Ethernet

La trama Ethernet, con muy pocas diferencias respecto a la 802.3, está formada por tres partes. En primer lugar, el encabezado, que comprende un preámbulo de 7 bytes que permite la sincronización. A continuación, un delimitador de inicio de trama (SFD - *Start Frame Delimiter*), de 1 byte, que indica el inicio de la información que de entrada tiene las direcciones origen y destino. El campo EtherType, de 2 bytes, indica el protocolo de capa superior que se utiliza. No existe en 802.3, y su utilización permite no considerar el uso de LLC. Por ejemplo, este campo informa el valor 800 para TCP/IP.

El campo de datos, que contiene la información de nivel 3, debe tener un tamaño mínimo de 46 bytes. Si es preciso, se añaden algunos bits de relleno (*padding*) para obtener este valor. El tamaño máximo de este contenido es de 1500 bytes, y se denomina *Maximum Transfer Unit*(MTU). Finalmente, un código de control de error *Cyclic Redundancy Check* (CRC) indica el delimitador de fin de tama *Frame Sequence Check* (FSC).

Preámbulo + SFD	Dirección origen	Dirección destino	Datos	FSC

Token Ring e IEEE 802.5

El protocolo de red cableada local Token Ring ha estado respaldado mucho tiempo por su fabricante, IBM. Su competidor, Ethernet, menos costoso y fácil de utilizar, aunque menos eficaz, ha acabado por reemplazarlo.

Aún podemos encontrar esta red, estandarizada como 802.5 por IEEE, en infraestructuras importantes y antiguas. Pero cada vez es menos frecuente.

1. Configuración de la red

La norma 802.5 se basa en el método del paso de testigo en una topología de anillo. Hay distintas combinaciones posibles para los anchos de banda, 4 Mbps, 16 Mbps y 100 Mbps, en función del cableado utilizado, UTP, STP o fibra multimodo.

Los equipos se conectan en estrella (topología física) al *Multistation Access Unit* (MAU).

Los MAU más antiguos disponen de tomas macho y hembra y se utilizan conectores DB9 para conectar las tarjetas a los MAU, a través de un cable Token Ring específico.

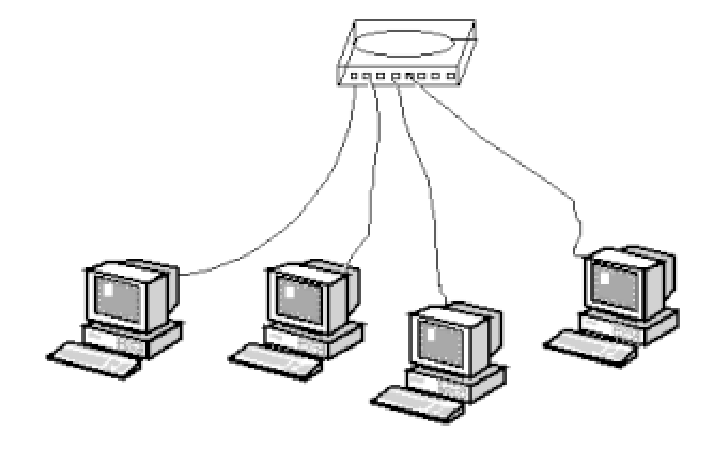


MAU



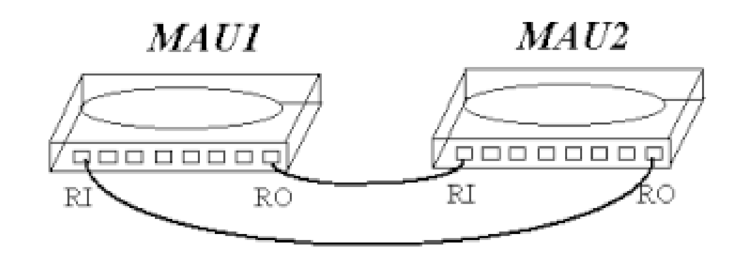
Cable Token Ring

La topología lógica es en anillo punto a punto, donde cada máquina actúa como repetidor.



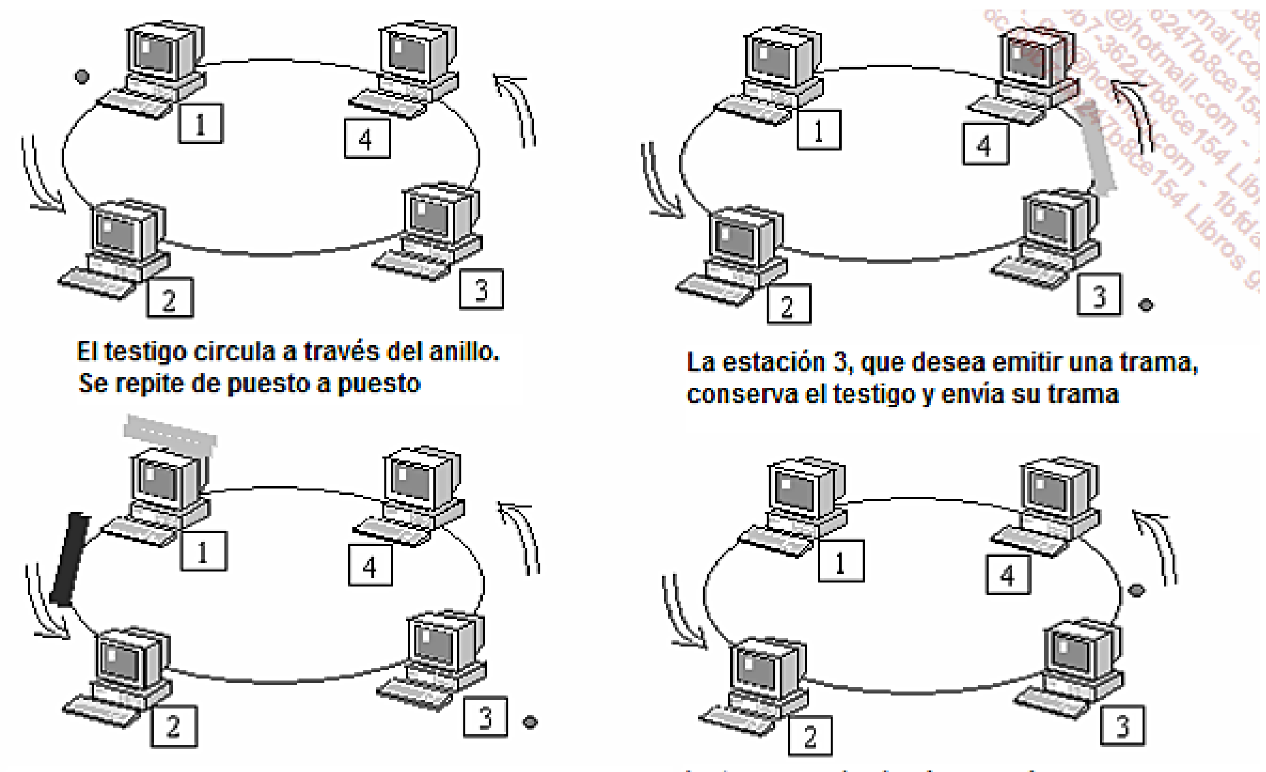
Topología física en estrella

Los MAU pueden interconectarse entre ellos, agrandando así el anillo principal, que utiliza los dos puertos *Ring In* (entrada en el anillo) y *Ring Out* (salida del anillo). Las tramas circulan en el sentido RI - RO.



Según el tipo de MAU utilizado, estos pueden repetir las señales o no hacerlo. El direccionamiento MAC de Token Ring se basa en un formato particular directamente vinculado a la topología y al algoritmo *Source routing* utilizado por los puentes.

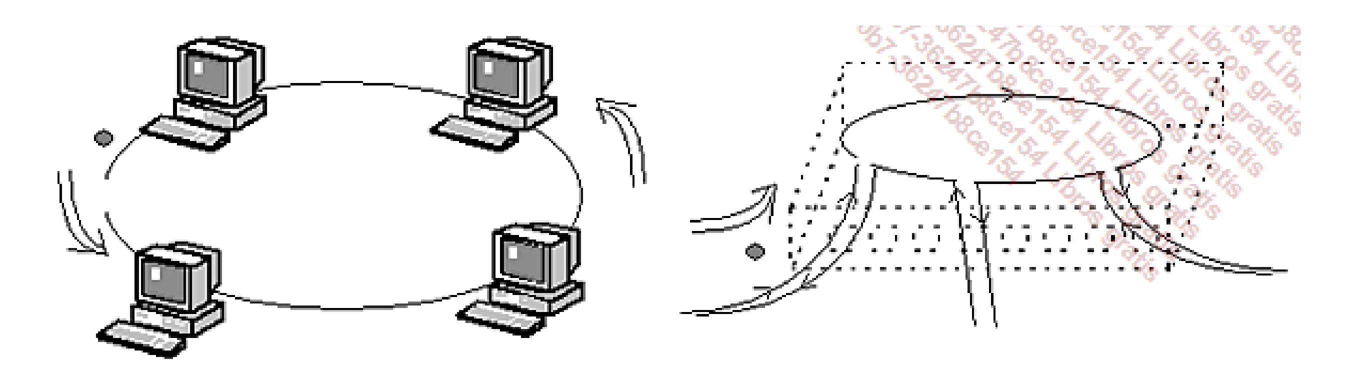
Desde un punto de vista lógico, una vez los equipos están conectados al MAU, ocurre como si los ordenadores estuvieran conectados entre ellos en topología de anillo punto a punto:



Además, es posible que un equipo reserve el próximo testigo con un determinado nivel de prioridad. Así pues, el testigo regenerado solo lo podrá utilizar un equipo que disponga del nivel de prioridad adecuado (o al menos igual al del testigo). Sin prioridad, el primer equipo por el que pasa el testigo es el que lo utiliza.

La implementación a 16 Mbps trabaja como FDDI, en el sentido de que el testigo se vuelve a emitir inmediatamente después del envío de la trama.

Desde un punto de vista lógico, el testigo se transmite de ordenador a ordenador. Desde un punto de vista físico, cada conexión de par trenzado permite añadir un ordenador, ampliando el anillo punto a punto.



Circulación del testigo en un anillo

Los MAU integran tolerancia a errores. Se configuran para prevenir una avería en un equipo (desconexión automática del anillo).

Un anillo Token Ring puede conectar hasta 260 equipos a 4 Mbps (136 equipos a 16 Mbps) y la longitud aconsejada entre lóbulos (conexión de los equipos a los MAU) es de 45 metros en UTP y 100 metros en STP.

El soporte utilizado son dos pares trenzados blindados (p. ej., tipo 1) o fibra óptica. Los tipos de conectores son DB9 para las tarjetas de red y tomas macho/hembra para la conexión a los MAU.

El tipo de codificación utilizado es Manchester diferencial.

La distancia entre dos MAU no puede superar los 45 metros con UTP, 200 metros con STP o hasta 1 km con fibra.

El alcance máximo de la red Token Ring, es decir, la longitud máxima del anillo principal (teniendo en cuenta la distancia MAU - equipo) varía según el número de MAU, repetidores y el tipo de localizaciones conectadas. Los distintos fabricante ponen a disposición tablas de cálculo para contabilizar el tiempo de propagación de una trama, dependiendo de la longitud máxima del anillo.

La longitud mínima de una trama es de 21 bytes y puede llegar a los 4.493 bytes a 4 Mbps y 18.000 bytes a 16 Mbps.

2. Autorreconfiguración del anillo

Un punto importante en Token Ring es la gestión del anillo mediante un equipo dedicado (aquel que lleve más tiempo conectado ya que este hecho le proporciona la dirección MAC más alta): el supervisor activo. Este equipo se encarga de solucionar una serie de problemas, como:

- La detección de la pérdida del testigo (cuando inesperadamente desaparece la estación que posee el testigo).
- La eliminación de una trama que completó su ciclo (el emisor desaparece antes de eliminar su trama del anillo).
- La detección de los errores en los mecanismos de prioridad (un testigo no debe generarse con la misma prioridad dos veces seguidas, salvo si su prioridad es la más baja).

Cada siete segundos, aproximadamente, el supervisor activo efectúa la comprobación del buen funcionamiento del conjunto, transmitiendo un testigo a su vecino inmediato. Cada equipo repite el testigo y a su paso guarda la dirección del supervisor activo, así como la dirección de su antecesor. Cuando el supervisor recupera el testigo, la prueba ha tenido éxito.

Debemos tener en cuenta que el problema puede generarse en el propio supervisor activo, que por ejemplo se puede detener inesperadamente. Si una estación no tiene más notificaciones de su predecesor, al cabo de siete segundos toma la iniciativa de enviar un mensaje a través del anillo con la siguiente información: su propia dirección, la dirección de su predecesor, que no ha notificado y el tipo de problema detectado. Este proceso permite aislar las partes del anillo que plantean problemas. Durante el proceso, cada tarjeta Token Ring se desconecta del anillo y realiza pruebas internas para saber si ella es el origen del problema. Si no se detecta ningún problema, la tarjeta se vuelve a instalar automáticamente en el anillo. En cualquier otro caso, el administrador deberá configurar manualmente la tarjeta para que funcione de nuevo en la topología.

Wi-Fi e IEEE 802.11

Las conexiones inalámbricas de tipo Radio LAN (RLAN) encontraron estándares adecuados gracias a los trabajos de los grupos IEEE 802.11.

1. Presentación

En 1997 el grupo de trabajo 802.11 estandariza, después de varios años de trabajo, la definición de redes de tipo Wireless LAN, que se retocó en 1999. Como en el caso de 802.3, estas especificaciones cubren las capas Física y Conexión de datos del modelo OSI. Esta última está dividida en dos subcapas: *Medium Access Control* (MAC), para el acceso al soporte de transmisión, y *Logical Link Control* (LLC), para el control de la transmisión.

En la capa Física, 802.11 define tres modos de transmisión. El primero está basado en la difusión infrarroja, que finalmente no se utilizará en las implementaciones de estas especificaciones. Las otras dos tecnologías utilizan la transmisión por radio. Finalmente, una sola, denominada *Direct Sequence Spread Spectrum* (DSSS), se implementará.

Las especificaciones 802.11 interesan tanto a algunos fabricantes que en 1999 forman la asociación *Wireless Ethernet Compatibility Alliance* (WECA). Su objetivo no es solamente promover este nuevo estándar, sino tambíen certificar dispositivos con el fin de garantizar su buen funcionamiento. El certificado *Wireless Fidelity* (Wi-Fi), patente de interoperabilidad, se otorga después de algunas pruebas. Finalmente, este organismo se rebautiza como Wi-Fi Alliance.

Después de las pruebas de compatibilidad, el fabricante del hardware puede etiquetar las cajas con el siguiente logotipo, siempre que respete los estándares exigidos.



Logo Wi-Fi

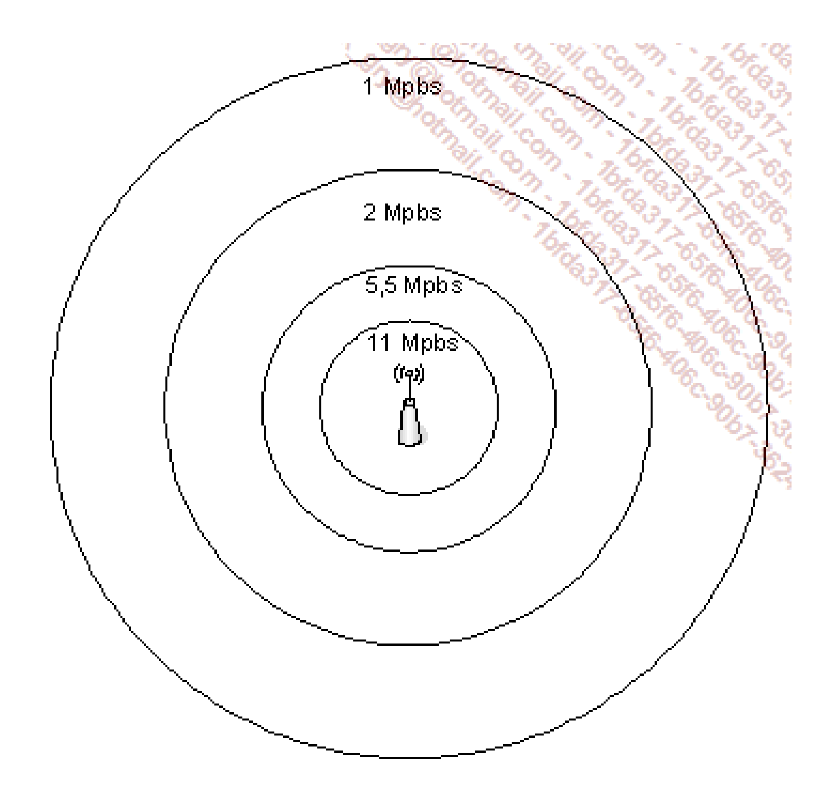
El estándar Wi-Fi permite la conectividad a distancias que superan algunas decenas de metros. La utilización de antenas permite alcanzar varios centenares de metros.

2. Normas de la capa Física

Hay muchas especificaciones que se han basado en la 802.11 original, de las cuales tres definen el uso de la capa física.

a. 802.11b

Esta norma, publicada en septiembre de 1999, aumenta la velocidad máxima de transmisión a 11 Mbps, con velocidades que pueden llegar a 5,5, 2 y 1 Mbps. La frecuencia de trabajo es de 2,4 GHz.



Rangos de velocidad disponibles (802.11b)

A partir de ahora, la red tiene un nombre, el SSID (*Service Set IDentifier*).

b. 802.11a

Como 802.11b, la norma 802.11a se publicó en septiembre de 1999. Pero, en cambio, su capa Física puede trabajar a 5 GHz. La transmisión máxima es de 54 Mbps. Como en la anterior, las velocidades pueden ser a 48, 36, 24, 18, 12, 9 y 6 Mbps.

A causa del cambio de frecuencia, las antenas 802.11a son incompatibles con las de 802.11b.

c. 802.11g

Este estándar, ratificado en junio de 2003, es el sucesor del 802.11b. También utiliza la banda de los 2,4 GHz y permite velocidades de 54 Mbps. Las velocidades posibles son las mismas que en 802.11a, es decir, 48, 36, 24, 18, 12, 9 y 6 Mbps.

d. 802.11n

La especificación 802.11g sigue siendo, desde 2003, la más explotada comercialmente. IEEE ha finalizado la evolución 802.11n en septiembre de 2009.

Después de las versiones 1.0 y 1.1, el grupo de trabajo de IEEE adoptó, en marzo de 2007, la versión 2.0 del borrador, que se acerca al estándar definitivo. En términos de capacidad, 802.11n en versión borrador incluía ya la calidad del servicio (QoS - *Quality of Service*), WMM (*Wi-Fi MultiMedia*) para las aplicaciones de VoIP (*Voice over IP*) y el *streaming*.

Las evoluciones que se tenían que definir eran importantes, ya que se trataba de mejorar a la vez, considerablemente, la velocidad y la cobertura de radio. Se pusieron en marcha varios procedimientos y fue difícil garantizar sus definiciones en el ámbito del estándar.

En primer lugar, se realizó un trabajo sobre la señal (capa Física). Este avance permitió prever una velocidad de 65 Mbps en lugar de los 54 Mbps de las especificaciones anteriores.

La segunda mejora en las transmisiones la han realizado una serie de técnicas relativas a la tecnología MIMO (*Multiple Input Multiple Output*). Por multiplexado espacial, se pueden tratar

simultáneamente hasta 4 flujos en lugar de uno solo. Utilizando más antenas de recepción que flujos, es posible recibir señales de varios caminos.

La especificación 802.11n utiliza bandas de frecuencia de 2,4 y 5 GHz. Con esta última, es posible duplicar la longitud del canal, lo que permite ganar aún más velocidad. La velocidad máxima de la versión final de 802.11n es de 200 Mbps. Las técnicas utilizadas permiten en teoría alcanzar los 540 Mbps.

El alcance en interiores es de 50 metros y de 125 metros en exteriores.

3. Hardware

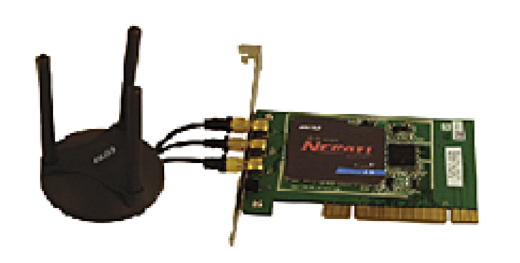
La elección del hardware Wi-Fi requiere, en primer lugar, asegurarse de su compatibilidad con la norma de la capa Física.

a. La tarjeta de red

Una adaptador Wi-Fi está compuesto por un chip conectado a una antena. Está integrado al equipo informático, ordenador portátil, PDA... o incluido en una tarjeta periférica.

En el caso de una solución integrada, la antena también lo está. Por ejemplo, en un ordenador portátil se coloca a lo largo de la pantalla. Los fabricantes también pueden adoptar la tecnología Intel Centrino, que incluye Wi-Fi en una solución integral.

Hay muchos modelos de tarjetas Wi-Fi que permiten incorporar esta función a un ordenador. Existen los formatos PC Card/PCMCIA, Compact Flash, PCI o USB.






Tipos de tarjetas Wi-Fi

b. El equipo de infraestructura

Se utilizan principalmente dos dispositivos. Su objetivo es la interconexión de la red Wi-Fi a la red cableada Ethernet, lo que se denomina sistema de distribución (DS - *Distribution System*).

Punto de acceso

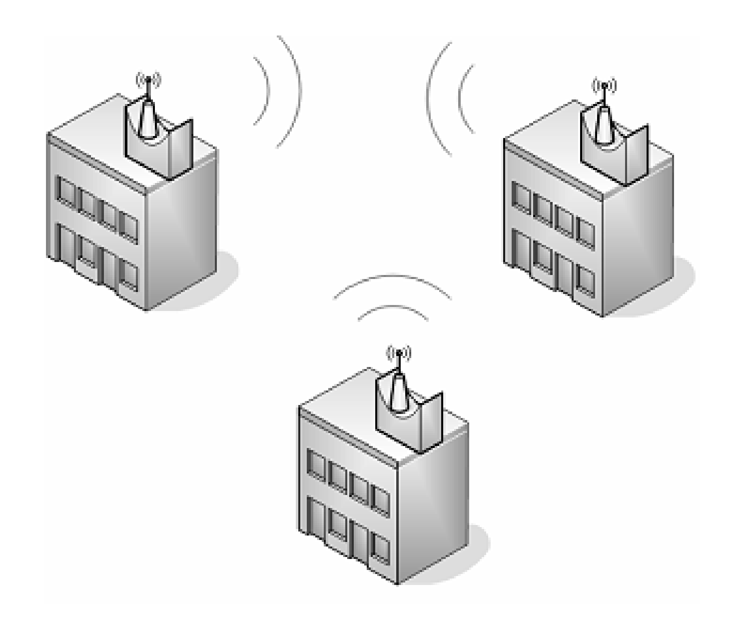
El punto de acceso (AP - *Access Point*) es el principal componente de la infraestructura de una red Wi-Fi. Como concentrador, centraliza todas las comunicaciones de los equipos que están asociados.



Concentradores Wi-Fi

Puente

La función principal de un puente (*bridge*) Wi-Fi es interconectar dos redes cableadas Ethernet a través de la interfaz inalámbrica. Los puentes Wi-Fi ofrecen una solución de bajo presupuesto para conectar las redes Ethernet de diferentes edificios, sin tener que recurrir a la fibra óptica, que, por supuesto, es más rápida.



c. Los dispositivos Wi-Fi

Los terminales Wi-Fi más frecuentes siguen siendo los ordenadores, sobre todo los portátiles, y los dispositivos móviles, como los asistentes personales (PDA). En las oficinas, otros dispositivos se comunican ya por Wi-Fi: videoproyectores, impresoras, cámaras…

A nivel industrial o en almacenes, los lectores de código de barras, que hace mucho que son inalámbricos, han adoptado el estándar Wi-Fi.



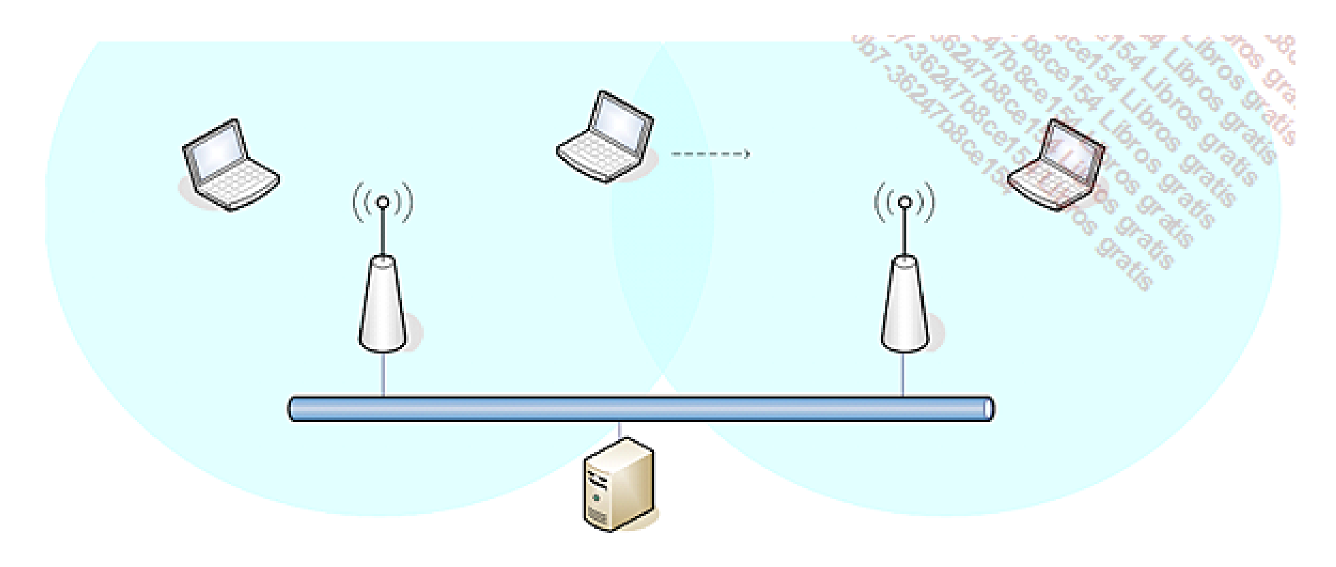
El éxito de la telefonía IP (VoIP) ha llevado a los fabricantes a ofrecer soluciones inalámbricas sobre la red Wi-Fi (VoWi-Fi). Estas recurren actualmente a funcionamientos propietarios, por ejemplo para la itinerancia, miestras se esperan los estándares.

4. Arquitectura

La primera arquitectura definida en la norma 802.11 permite una comunicación de igual a igual entre al menos dos equipos. Se denomina *Independent Basic Service Set* (IBSS), y se utiliza para crear redes *ad hoc*.

La segunda arquitectura requiere un punto de acceso. En este caso *Basic Service Set* (BSS) actúa como administrador para las estaciones periféricas que se le asocian. Todas las comunicaciones deben pasar por él.

Una red de mayor amplitud, con varios puntos de acceso, se llama *Extended Service Set* (ESS). Este tipo de red permite el desplazamiento por el interior de la empresa, asociándose sucesivamente a los puntos de acceso más cercanos y sin producir cortes de comunicación. Esta capacidad es la itinerancia o *roaming*.



Wi-Fi e itinerancia

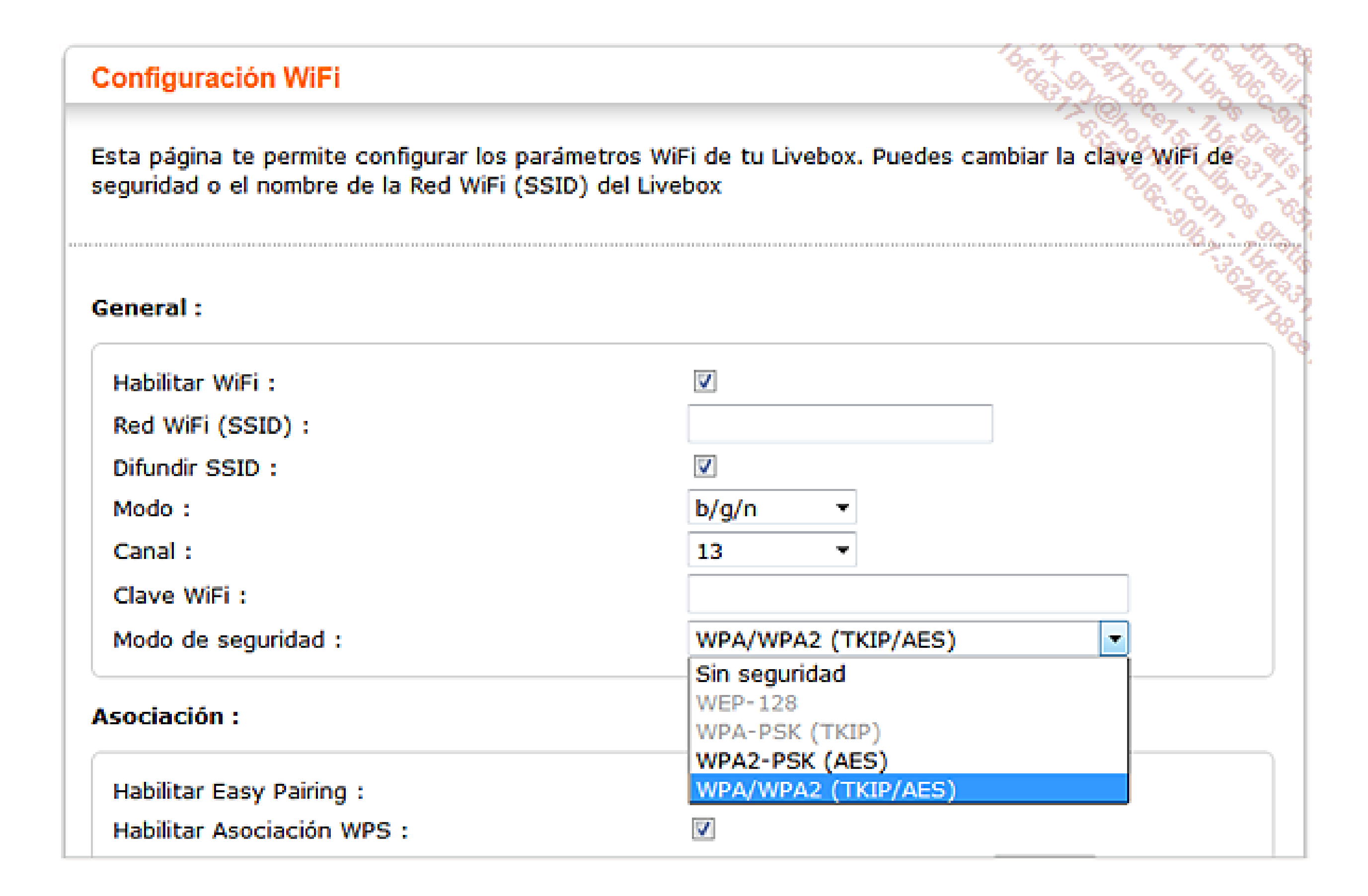
5. Seguridad

a. WPA

El Wi-Fi Protected Access se finalizó en 2003 en respuesta a las numerosas vulnerabilidades de WEP (*Wired Equivalent Privacy*). WPA implementa la mayor parte de las funcionalidades descritas en la norma 802.11i que se había completado totalmente en esa época.

El diseño del protocolo se basa en la utilización de un servidor de autenticación basado en 802.1X que es necesario para la distribución de claves para cada uno de los usuarios.

Existe una implementación más básica para particulares y pymes, que es la utilización de una clave compartida (*Pre-Shared Key* o PSK).



Ejemplo de elección de seguridad Wi-Fi en un router ADSL.

WPA se basa normalmente en el protocolo TKIP (*Temporal Key Integrity Protocol*), que utiliza claves más largas que las claves WEP. Este protocolo TKIP permite el intercambio dinámico de las claves.

Existen dos variantes de WPA (v1 o v2):

- WPA-personal.
- WPA-empresa.

El WPA-personal no necesita servidor de autenticación; cada equipo se autentica directamente con el punto de acceso a través de una clave de 256 bits.

La versión para empresas se basa en la utilización de un servicio RADIUS (*Remote Dial In User Services*) y se apoya necesariamente en un cifrado AES (*Advanced Encryption Standard*).

De este modo, WPA garantiza no solamente la autenticación, sino también el cifrado. Igualmente protege la integridad de las tramas firmándolas. Así, es casi imposible realizar ataques de modificación de las tramas y de su CRC (*Cyclic Redundancy Check*) como con WEP. Ofrece igualmente un mecanismo para contar tramas que impide la repetición por parte de los atacantes.

El algoritmo utilizado por la identificación de los mensajes es el MIC (*Message Integrity Code*), llamado también «Mickeal».

b. WPA2

Se trata de la versión del protocolo que respeta escrupulosamente la norma IEEE 802.11i.

El cifrado se implementa a través del protocolo AES.

Desde 2006, es obligatoria la compatibilidad WPA2 para los equipos certificados Wi-Fi.

6. Utilización

En primer lugar se debe considerar esta tecnología como la versión inalámbrica de Ethernet. Se presenta como la respuesta a las exigencias de movilidad dentro de las empresas. Más allá del uso administrativo, que se traduce en un equipo colocado en una mesa, Wi-Fi permite una verdadera itinerancia.

Otra utilización importante es la extensión de la red en la empresa. Llevar la red local allí donde aún no está disponible es, a partir de ahora, mucho más fácil que teniendo que llevar el cable. Además de la facilidad y rapidez de la implementación, el coste representa un criterio de elección importante.

Un *Hot-Spot* permite un acceso a Internet a través de la tecnología Wi-Fi. También se le conoce con el nombre de Acceso Público a Internet (API).

7. Encabezado de trama Wi-Fi

La capa *Medium Access Control* (MAC), capa inferior base de la Conexión de datos, constituye el núcleo de Wi-Fi.

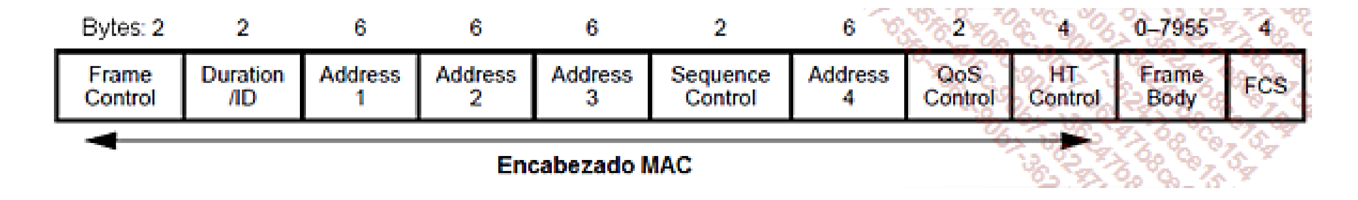
Esta capa debe administrar los canales de comunicación o, más bien, la ausencia de canales de comunicación físicos, caracterizados por una frecuencia de radio. Este canal debe compartirse entre los distintos nodos de la red. Cada uno posee su propia dirección MAC, como en Ethernet.

El mecanismo de gestión de los soportes de comunicación no puede utilizar la detección de colisiones, impensable en una red inalámbrica. Por ello se utiliza una solución que evita las tramas de tipo CSMA/CA.

La gestión de la división del ancho de banda no es, ni mucho menos, la única utilización de la capa MAC. Antes de emitir datos hacia un punto de acceso, un equipo debe conectarse a *Basic Service Set* (BSS), la red del equipo administrador. Pero antes será necesario un proceso de asociación, y antes de eso, puede que el punto de acceso pida la autentificación del equipo.

También pueden presentarse otras problemáticas a este nivel. Se gestionan la fragmentación/defragmentación de las tramas transmitidas, así como la administración de la capacidad para comunicar a distintas velocidades. Tampoco se deben olvidar los controles de error y el ahorro de energía. La seguridad también se puede administrar en la capa MAC.

El encabezado de trama Wi-Fi es claramente más complejo que su par Ethernet. El cuerpo de la trama tiene un tamaño máximo de 7956 bytes. Se observa que se reservan cuatro campos para las direcciones MAC. Esto permite el uso de las direcciones fuente y destino, y de puntos de acceso como intermediarios.



Construcción de un encabezado de trama Wi-Fi

El proyecto de enmienda 802.11n draft, entre otras cosas, ha dado como resultado algunas modificaciones en la capa MAC, tanto en el formato del encabezado como en su contenido. Se ha añadido un campo destinado a la calidad del servicio (QoS - *Quality of Service*) después de la Dirección 4.

Bluetooth e IEEE 802.15

El éxito de las tecnologías de red que utilizan la radio se confirma con Bluetooth, que se ha convertido en el estándar comercial de las redes de tipo RPAN (*Radio Personal Area Network*) y otras comunicaciones entre dispositivos.

1. Antecedentes

Lanzado en 1994 por la empresa Ericsson, esta tecnología lleva el nombre de un rey danés, Harald II. Apodado Harald II Blåtand (diente azul - *blue tooth*), fue un gran consumidor de arándanos que unificó Dinamarca, así como una parte de Suecia y Noruega, en el siglo IX. Este nombre señala la voluntad, por parte de Ericsson, de unificar el mundo de la telefonía móvil.

Otros grandes fabricantes, como Nokia, Intel, Microsoft, Toshiba e IBM, se unieron a Ericsson a partir de 1998 para formar la Bluetooth *Special Interest Group* (SIG), que actualmente cuenta con más de 10.000 miembros.



Logo Bluetooth

Destinado a permitir la comunicación entre equipos muy heterogéneos y poco distantes, Bluetooth integra, en un chip de menos de un centímetro, características muy avanzadas.

2. Estandarización

La especificación 1.0, publicada en julio de 1999, se adapta a las transmisiones de voz, datos e imágenes. Su velocidad teórica es de 1 Mbps. Su frecuencia de trabajo es la misma que la de Wi-Fi, 2,4 GHz; es muy económica en cuanto a energía. La segunda especificación data de finales del año 2004. Es todavía más económica en términos energéticos y, teóricamente, alcanza velocidades de 10 Mbps, lo que permite la transmisión de vídeos.

El grupo IEEE 802.15 (WPANWG - *Wireless Personal Area Network Working Group*) eligió basarse en Bluetooth para su estándar. De hecho, se formaron 4 subdivisiones entre los grupos de proyecto o Tasks Groups.

Del proyecto 802.15.1, publicado en junio de 2002, ha resultado un estándar basado en Bluetooth v1.1.

El segundo, 802.15.2, que finalmente no ha salido a la luz, tenía como misión la coexistencia entre WPAN (802.15) y WLAN (802.11).

La solución de alta velocidad (HR - *High Rate*) del grupo 802.15.3 se finalizó en junio de 2003. Permite la transferencia de archivos de vídeo y audio en *streaming*, basándose en la tecnología*Ultra Wide Band* (UWB), procedente del ejército estadounidense. Este estándar es capaz de alcanzar velocidades de varios cientos de megabits por segundo, a una distancia de varias decenas de metros. Además, esta solución permite atravesar obstáulos, como los muros de un edificio.

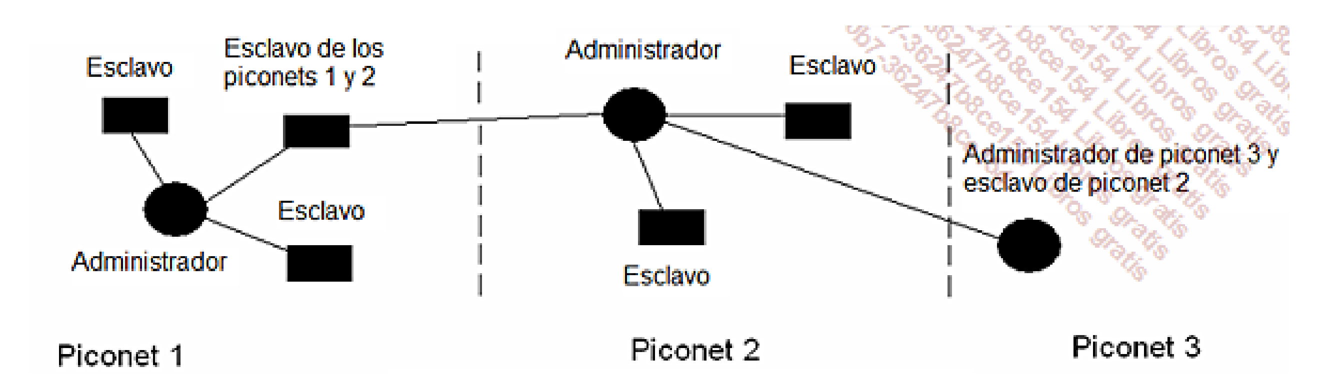
Finalmente, en el otro extremo, la solución de baja velocidad, con un importante ahorro de energía, la del grupo 802.15.4, se aprobó en 2006. Esta norma, también llamado ZigBee, es la prolongación de HomeRF y puede utilizarse para transmitir comandos en lugar de datos. Su velocidad es de 250 Kbps como máximo a una distancia de unos 10 metros.

3. Red Bluetooth

Los equipos Bluetooth pueden interconectarse de dos maneras.

La primera consiste en formar una única red, el *piconet*, que comprende un terminal administrador que asume hasta 7 terminales esclavos. Todas las comunicaciones, incluso entre esclavos, se administran y transitan por el administrador.

Una segunda solución es interconectar varias redes en estrella. Estas forman una *scatternet*, en la cual el administrador de un *piconet* puede convertirse en el esclavo de otro *piconet*.



En estos esquemas, se suministran distintas velocidades entre equipos, para un total de 1 Mbps en la especificación 1.0. Una comunicación bidireccional *full-duplex* alcanzará alrededor de 434 Kbps en cada sentido, mientras que otra que esté desequilibrada alcanzará 732 Kbps en un sentido y 58 Kbps en el otro.

Bluetooth en realidad se diseñó para diferentes propósitos. Las funcionalidades de un dispositivo forman un repertorio de perfiles. Para que dos dispositivos se puedan comunicar, deben utilizar la misma funcionalidad. Entre los diferentes perfiles, podemos citar:

- GAP (*Generic Access Profile*), que define los procedimientos de búsqueda de dispositivos, de conexión y de seguridad.
- HS Profile (*Headset Profile*), para los kits de manos libres.
- LAN Access Profile.
- Fax Profile.
- FTP (*File Transfer Profile*).
- CTP (*Cordless Telephony Profile*)...

Una red TCP/IP de radio entre diferentes máquinas (*Ad hoc*) se puede construir gracias al perfil de red local de Bluetooth.

4. Clases de equipos

Existen tres clases de dispositivos Bluetooth:

- Clase 1, de una potencia de 100 mW, para grandes distancias, de 100 metros.
- Clase 2, de una potencia de 2,5 mW, para distancias medias, de entre 15 y 20 metros.
- Clase 3, de una potencia de 1 mW, para pequeñas distancias, alrededor de 10 metros.

La mayor parte de los equipos comercializados son de clase 3. Esta tecnología se utiliza mucho para kits universales de manos libres para teléfonos móviles. También se encuentra en conexiones entre dispositivos (PDA...) o entre ordenadores y periféricos (impresoras...). En este último caso, sustituye a los cables USB.



Ejemplos de dispositivos que utilizan Bluetooth

Otras tecnologías

En las capas bajas de las redes pequeñas, se pueden encontrar otras tecnologías. Entre ellas, el Bucle Local Eléctrico (BLE, más conocido como PLC) parece una prometedora tecnología alternativa a la LAN.

1. Otros estándares de IEEE

Se han abandonado algunos grupos de trabajo (p. ej., 802.4, 802.6, 802.7, 802.9, 802.10 y 802.12), mientras que se han creado otros a medida que evolucionan las tecnologías.

IEEE 802 LAN/MAN Standards Committee

IEEE 802 Working Group & Executive Committee Study Group Home Pages

Active Working Groups and Study Groups

- 802.1 Higher Layer LAN Protocols Working Group
  - Link Security Executive Committee Study Group is now part of 802.1
- 802.3 Ethernet Working Group
- 802.11 Wireless LAN Working Group
- 802.15 Wireless Personal Area Network (WPAN) Working Group
- 802.16 Broadband Wireless Access Working Group
- 802.17 Resilient Packet Ring Working Group
- 802.18 Radio Regulatory TAG
- 802.19 Wireless Coexistence Working Group
- 802.20 Mobile Broadband Wireless Access (MBWA) Working Group
- 802.21 Media Independent Handover Services Working Group
- 802.22 Wireless Regional Area Networks
- 802.23 Emergency Services Working Group

Inactive Working Groups and Study Groups

- 802.2 Logical Link Control Working Group

Disbanded Working Groups and Study Groups

- 802.4 Token Bus Working Group (material no longer available on this web site)
- 802.5 Token Ring Working Group

Extracto del sitio web de IEEE donde se puede ver el estado de los diferentes estándares

Vamos a examinar estos nuevos grupos que se han definido y los temas que cubren.

a. 802.16

Este grupo de trabajo se centra en el desarrollo de los estándares y mejoras para soportar y desarrollar las redes inalámbricas de tipo MAN (*Metropolitan Area Network*). Una de las aplicaciones es WiMAX, que se describe en el capítulo Protocolos de redes MAN y WAN - sección Interconexión de la red local.

Puede encontrar información adicional en el sitio web: http://www.ieee802.org/16/

b. 802.17

En el caso de redes de tipo MAN o WAN, se utiliza ampliamente la fibra óptica en topologías en anillo. Estos anillos utilizan protocolos que no están optimizados, ni son adaptables a las peticiones bajo demanda de diferentes características, como «la velocidad de implementación», la asignación del ancho de banda y de la velocidad, la reducción de costes de hardware y de administración.

El grupo de trabajo *Resilient Packet Ring* contribuye al desarrollo de los estándares y al despliegue de ofertas adaptables alrededor de la fibra óptica en anillo.

Puede encontrar información adicional en el sitio web: http://www.ieee802.org/17/

c. 802.18

Este grupo de trabajo centra su actividad en la normalización de las comunicaciones radioeléctricas.

Puede encontrar información adicional en el sitio web: http://www.ieee802.org/18/

d. 802.19

Este grupo se ocupa de la cohabitación con otros estándares inalámbricos.

Puede encontrar información adicional en el sitio web: http://www.ieee802.org/19/

e. 802.20

Este grupo se ocupa de los accesos inalámbricos de un gran ancho de banda.

Puede encontrar información adicional en el sitio web: http://www.ieee802.org/20/

f. 802.21

Este grupo se ocupa de la interoperabilidad entre dispositivos heterogéneos basados en tipos de red distintos.

Puede encontrar información adicional en el sitio web: http://www.ieee802.org/21/

g. 802.22

Este grupo de trabajo se ocupa de las redes regionales inalámbricas.

Puede encontrar información adicional en el sitio web: http://www.ieee802.org/22/

h. 802.23

El objetivo de este grupo es definir un ámbito independiente del soporte, que responde a las exigencias de las autoridades civiles, en el contexto de los sistemas de comunicaciones.

Puede encontrar información adicional en el sitio web: http://www.ieee802.org/23/

2. Infrared Data Association (IrDA)

Con la utilización del soporte infrarrojo, IrDA define una secuencia de protocolos que permiten garantizar la comunicación entre dispositivos. Existen dos normas principales IrDA.

a. El protocolo IrDA DATA

IrDA DATA es un estándar de intercambios bidireccionales, adaptado a la transferencia de datos. Tiene múltiples aplicaciones: ordenadores, impresoras, asistentes personales, teléfonos móviles y potencialmente cualquier dispositivo móvil.



Está compuesto por una serie de protocolos obligatorios:

PHY (físico): dependiendo de la potencia eléctrica utilizada, este protocolo garantiza una comunicación a 2 metros como máximo entre dispositivos. Las versiones de escaso consumo de energía permiten el intercambio de información a una distancia máxima de 20 cm y hasta 30 cm si el destino es un dispositivo estándar. Este protocolo garantiza la comunicación bidireccional a una velocidad de entre 9,4 Kbps y 4 Mbps. Los paquetes de datos se protegen gracias a un CRC.

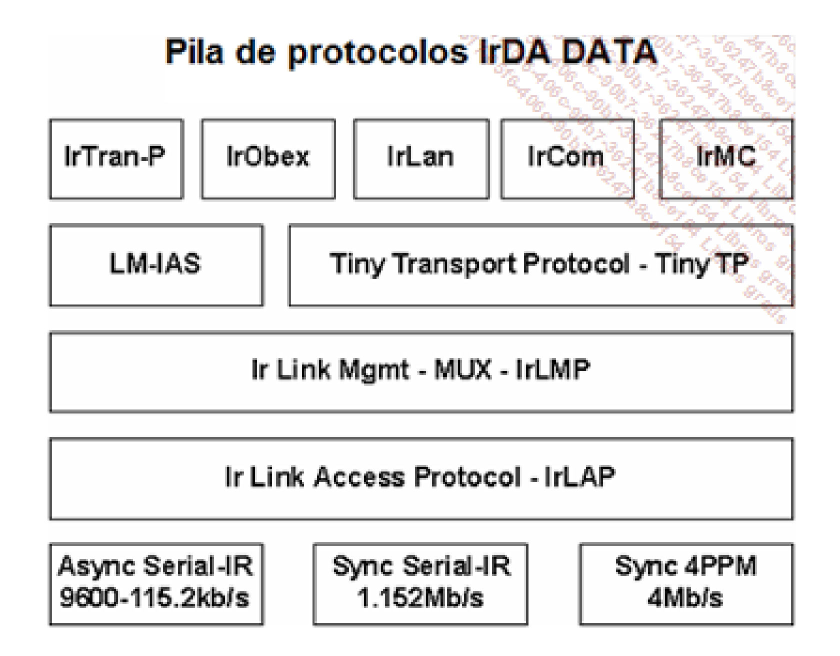
IrDA Link Access Protocol (IrLAP): este protocolo administra la conexión entre dispositivos garantizando una trasferencia de datos ordenada y fiable. También se encarga de la localización automática de dispositivos.

IrDA Link Management Protocol (IrLMP): este protocolo asegura el multiplexado, permitiendo la utilización de diferentes canales a nivel IrLAP. Como este último, se encarga de la localización automática, pero solo para los protocolos y servicios.

Según su utilización, se aplican algunos protocolos opcionales:

- Tiny TP, controla el flujo IrLMP de segmentación y de montaje.
- IrCOMM, emulación de puertos COM.
- IrOBEX, servicios de intercambio de objetos.
- IrDA Lite, métodos de disminución de código, garantizando la compatibilidad con todas las especificaciones IrDA.

- IrTan-P, protocolo de intercambio de imágenes.
- IrMC, especificaciones de intercambios entre dispositivos de telefonía e informáticos (directorios, calendarios...).
- IrLAN, acceso a redes locales.



b. El protocolo IrDA CONTROL

Este estándar define los intercambios entre dispositivos (teclado, ratón, *joystick*...). Se compone de tres protocolos obligatorios.

PHY (físico): asegura una comunicación bidireccional a una velocidad de 75 kbps, para una distancia máxima de 5 metros. Los paquetes de datos se protegen gracias a un CRC. Este protocolo está optimizado para componentes de escaso consumo energético.

MAC: permite la comunicación simultánea entre dispositivos (hasta 8) y tiempos de respuesta breves. Asegura el direccionamiento dinámico de los dispositivos (*asymmetric*MAC).

LLC: detecta los errores y transmite los datos.

La aplicación de las tecnologías IrDA aún no está totalmente adaptada para las redes informáticas, a causa de la limitación de velocidad impuesta por el soporte y su relativa sensibilidad a las interferencias, al contrario de lo que ocurre con las tecnologías que utilizan ondas de radio.

3. Bucle Local Eléctrico (BLE)

a. Principios

La transmisión a través del Bucle Local Eléctrico (BLE), en inglés *Power Line Communications*(PLC) o *Broadband Power Line* (BPL), existe desde los años cincuenta. La técnica utilizada en aquella época era unidireccional y solo obtenía velocidades bajas. Sigue siendo utilizada, por ejemplo, para el encendido y apagado del alumbrado público y la conmutación de los contadores eléctricos entre tarifas diurnas y nocturnas.

Hacia finales de los años noventa, las investigaciones permitieron al BLE convertirse en bidireccional y permitir velocidades más altas. Esta solución puede implementarse para comunicaciones dentro de edificios, o a distancias cortas. Otras utilidades, como el acceso a Internet por BLE, serán posibles a corto plazo. En España, se está legislando al respecto. La eléctrica que está más avanzada en este sentido es Endesa.

En el ámbito de la utilización de las líneas eléctricas para redes locales, se creó un consorcio en Estados Unidos llamado *HomePlug Powerline Alliance*. Agrupa a diferentes agentes del sector, como por ejemplo Intel, Linksys y Motorola, con el objetivo de trabajar en un marco estándar para el bucle local eléctrico.

Se han definido certificaciones y pruebas para comprobar la interoperabilidad de los componentes. Tras la validación, el fabricante tiene permiso para utilizar el logotipo correspondiente; por ejemplo, en la caja del hardware.





Logos HomePlug

La primera certificación fue HomePlug 1.0, que ofrecía velocidades teóricas de 14 y luego de 85 Mbps. A esta certificación inicial le sucedió HomePlug AV (HPAV), destinada a la red multimedia doméstica. Compatible con la versión 1.0, permite velocidades teóricas de 200 Mbps. Es más segura, y ofrece la calidad del servicio (QoS) y el *streaming* de audio y vídeo.

Las otras dos siglas corresponden a las especificaciones *HomePlug Access* BPL (*Broadband Power Line*), para el acceso de alta velocidad en las viviendas, y HomePlug CC (*Command & Control*) para el control de dispositivos (control de la iluminación, climatización...) a través de esta tecnología.

El consorcio HomePlug se acerca igualmente a IEEE y a su grupo P1901 (http://grouper.ieee.org/groups/1901), destinado a estandarizar este tipo de comunicaciones.

La norma común, que permite la interoperabilidad de los tres grandes sistemas CPL, se finalizó en 2010: IEEE STD 1901-2010. Esta norma prevé la utilización de adaptadores domésticos que pueden llegar, en teoría, a la velocidad de 500 Mbps.

b. El funcionamiento

Esta tecnología utiliza la red de instalación eléctrica de un edificio para transportar datos informáticos. Por ello se emplea una potencia mucho menor y altas frecuencias (banda 1,6 a 30 MHz) en los cables eléctricos. Los filtros permiten diferenciar esta señal superpuesta a los 220 V y 50 Hz, conservando solo los datos informáticos.

Esta señal es recibida por cualquier adaptador BLE conectado a la red eléctrica interna. A continuación, este dispositivo transforma el impulso en señal Ethernet, como el USB, al cual se puede conectar el ordenador.



Adaptador BLE

El transporte de frecuencias altas a través de los cables eléctricos puede plantear un problema de interferencias radioeléctricas. La potencia suministrada no debe ser demasiado elevada para no impedir el funcionamiento de los aparatos que no son de red. Además, estas interferencias pueden

tener como consecuencia una falta de seguridad en las comunicaciones. HomePlug prevé, por otra parte, el posible cifrado de los datos *Advanced Encryption Standard* (AES), que reemplaza a *Data Encryption Standard* (DES).

La capa física de HomePlug utiliza la modulación por intervalo de espectro, o *Spread Spectrum*, con la técnica de transmisión *Orthogonal Frequency Division Multiplexing* (OFDM). El modo de acceso es de tipo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). Estos medios también se utilizan en las comunicaciones Wi-Fi.

Aunque el BLE carece de normalización para la empresa, con velocidades un poco más altas, puede ser un buen complemento para Wi-Fi. De hecho, la interconexión de la red Wi-Fi con la troncal Ethernet no siempre es posible, por ejemplo por motivos de distancia. En tal caso, la implementación de una extensión con BLE puede proporcionar una gran flexibilidad.

Es muy probable que las evoluciones de esta prometedora tecnología permitan rápidamente un uso aún más interesante en la empresa, incluso en exteriores.

Interconexión de la red local

En los últimos años las solicitudes de interconexión entre empresas (lugares distantes) o a Internet han aumentado vertiginosamente. Tampoco los particulares se han quedado atrás.

Paralelamente, las tecnologías que facilitan estas conexiones han experimentado un progreso considerable. Muchas soluciones utilizan soportes públicos, como la línea de la Red Telefónica Conmutada (RTC) o el cable de fibra óptica, que también puede desplegarse en el marco de interconexiones privadas. Igual que las redes pequeñas, también las redes de radio evolucionan.

1. Utilización de la red telefónica

La red telefónica conmutada con cables de cobre sigue siendo el soporte principal de las comunicaciones más allá de la red local. Es, de hecho, poco común diseñar un edificio residencial o de oficinas sin esta interconexión de red.

Por lo general se ha destinado a las transmisiones de voz, pero es plenamente operativo desde un punto de vista técnico para transmitir datos.

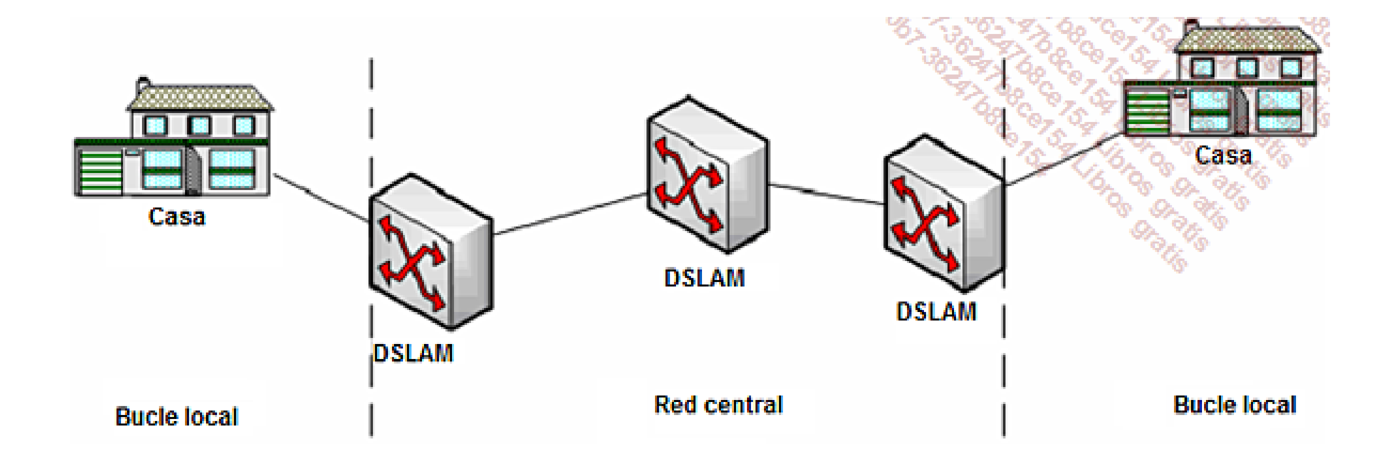
Podemos distinguir dos partes de la red telefónica conmutada. La primera, llamada bucle local (BL), es propiedad casi en su totalidad de Telefónica y conecta las centrales de este operador con los edificios de los clientes finales. Por encima de ella, una red central asume la comunicación.

La red central de Telefónica transmite la información en forma digital desde hace mucho tiempo. En primer lugar, la voz se codifica (muestreo). Antes de enviarse al bucle local del destinatario correspondiente, se descodifica. Esta red central no tiene ninguna dificultad en transmitir datos informáticos.

En el interior de las centrales, los equipos *Digital Subscriber Line Access Multiplexor* (DSLAM) interconectan al abonado con la red central del operador. Inicialmente, solo Telefónica instalaba DSLAM en sus propias centrales. Desde hace algunos años, otros operadores pueden instalar sus dispositivos e interconectar su red central (digital) al bucle local.

En este acceso desglosado parcial, la comunicación telefónica se sigue produciendo a través de los servicios de Telefónica, mientras que el operador alternativo se ocupa de la circulación de los datos. Un acceso desglosado total indica que el operador alternativo se encarga por completo de las comunicaciones. En este caso, el abono a Telefónica lo hace el operador alternativo, y no el cliente final.

En una zona de acceso no desglosado, la central solo contiene equipos de Telefónica.



Para transferir datos a través de la línea RTC, el módem analógico ha sido durante mucho tiempo la

solución más utilizada. Sin embargo, poco a poco ha caído en desuso y ahora se emplea sobre todo para proporcionar únicamente funcionalidades de fax. Los propios módems de la Red Digital de Servicios Integrados (RDSI) han sido abandonados por la adopción masiva en España de la *Asymmetric Digital Subscriber Line* (ADSL), aunque esta tecnología no está disponible en todos los lugares.

Otras técnicas, como las Líneas Dedicadas (LD), pueden beneficiarse de este soporte a través de la línea RTC.

2. Red digital de servicios integrados (RDSI)

a. Principios

La Red Digital de Servicios Integrados (ISDN - *Integrated Services Digital Network*) es un conjunto de normas establecidas por la ex-CCITT (ITU-T) para transformar la red telefónica conmutada (analógica en sus inicios) en una red digital mundial.

En España, Telefónica ofrecía un acceso RDSI para su red y lo comercializó con dicho nombre. Aunque compiten con otras tecnologías más recientas, las ofertas RDSI siguen estando presentes.

Una red completamente digitalizada permite la transmisión de cualquier tipo de información, voz, vídeo o datos. A través de la línea RTC se pueden ejecutar muchas aplicaciones: transferencia de archivos, videoconferencia, audioconferencia, fax.

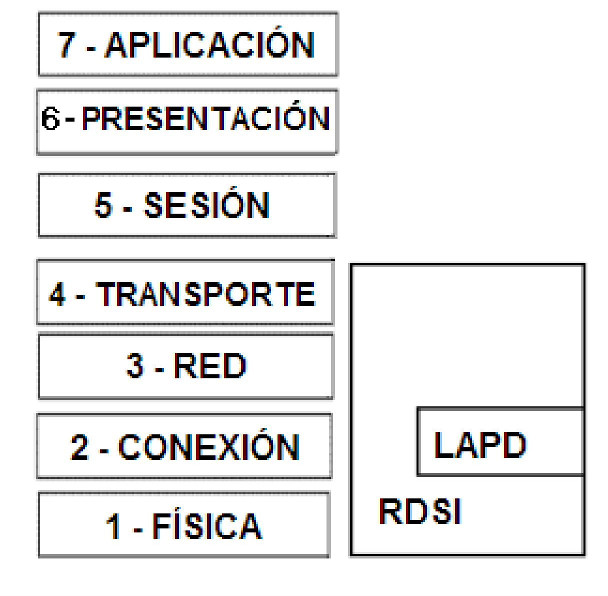
Como la RDSI es un estándar internacional, la compatibilidad entre países está garantizada.

b. Correspondencia con el modelo OSI

La RDSI cubre las tres primeras capas del modelo OSI. En la primera, la capa Física, la RDSI proporciona un multiplexado temporal entre los distintos elementos. Localmente, un módem RDSI permite la conexión entre el terminal y la red. Se utiliza el conector RJ45 y las interfaces S/T (S para el abonado, T para la red).

La capa de Conexión está garantizada por el protocolo *Link Access Protocol on the D-Channel Multipoint* (LAP-D), que implementa direcciones multipunto y de difusión, así como la gestión del canal D.

A nivel de la capa de Red, hay disponibles dos canales distintos. El llamado básico (Canal B) se utiliza para la transferencia de información. El canal de datos (Canal D) se utiliza para la digitalización, el establecimiento de la comunicación, la identificación del interlocutor y otros servicios.



RDSI y OSI

c. Tipos de acceso disponibles

Se han definido dos tipos de acceso para el usuario, en relación con la velocidad básica necesaria para transmitir la voz, 64 Kbps.

En Europa, la voz en la red telefónica se digitaliza a 8000 muestreos por segundo, es decir, 1 cada 125 microsegundos. Se define cada impulso en 8 bits (256 niveles posibles). Así, esta codificación de modulación por impulsos codificados (MIC) transmite a 64 Kbps. Esta unidad es la base de la RDSI.

El acceso básico incluye:

- 2 canales B a 64 Kbps cada uno (o sea 128 Kbps por agregación de línea), para la transmisión de los datos.
- 1 canal D a 16 Kbps para la señalización.

Gracias a la compresión RDSI, es posible alcanzar hsata 400 Kbps.

El acceso primario proporciona:

- 30 canales B a 64 Kbps cada uno.
- 1 canal D a 64 Kbps.

En EE. UU. y en Japón, el acceso primario corresponde a 1 canal D y a 23 canales B.

En España, por ejemplo, las ofertas comerciales son adaptaciones de estos accesos.

La RDSI es un servicio conmutado; por lo tanto, se factura al usuario en función de la duración de comunicación y la distancia recorrida. Por supuesto, también se tiene en cuenta el tipo de acceso.

3. Línea dedicada (LD)

a. Los principios

Una línea dedicada es permanente y se alquila forzosamente a un operador telefónico, en la mayoría de casos a Telefónica. Interconecta dos números predefinidos punto a punto. No es necesario marcar el número del destinatario.

La facturación depende de la distancia y la velocidad ofrecida.

Las líneas dedicadas son accesibles desde cualquier punto del planeta. Debido a su coste, es una solución que utilizan mayoritariamente las empresas.

Telefónica comercializa este servicio bajo el nombre Plan Novacom.

b. Velocidades

Con las líneas dedicadas, las velocidades son simétricas. En Europa se estandarizan con el nombre Ex y en EE. UU. con los niveles Tx.

Por ejemplo, las principales velocidades europeas son:

- E1, a 2.048 Mbps, equivalente 30*64 Kbps.
- E2, a 8.848 Mbps, equivalente 4*E1.
- E3, a 34.368 Mbps, equivalente 4*E2.
- E4, a 139.264 Mbps, equivalente 4*E3.

Entre las velocidades americanas, podemos citar:

- T1, a 1.544 Mbps, equivalente 24*64 Kbps.
- T2, a 6.312 Mbps, equivalente 4*T1.
- T3, a 44.736 Mbps, equivalente 7*T2.

4. Tecnologías xDSL

a. Principios

Anteriormente hemos visto que, a través del bucle local de la red telefónica conmutada, la señal se transmite habitualmente en forma analógica, y se transforma en digital a través del circuito troncal. Las tecnologías de transmisión, como la *Asymmetric Digital Subscriber Line*(ADSL), permiten utilizar las frecuencias no utilizadas por la señal analógica. Permiten velocidades digitales muy elevadas, forzando el cable de cobre hasta el máximo de sus posibilidades.

De esta manera, se obtienen velocidades proporcionales, pero en distancias cortas dentro del bucle local. De hecho, la pérdida de calidad de esta señal a través del cable de cobre es muy rápida.

Para que una línea telefónica sea apta para una conexión ADSL, el abonado debe estar situado como máximo a 5 kilómetros de la central a la cual se conecta. Con ADSL 2+, esta distancia se incrementa alrededor de 1,5 kilómetros. No todo el mundo se puede conectar a alta velocidad a Internet mediante ADSL.

En casa del abonado, un módem específico permite dar el formato adecuado a la señal antes de enviarla por el soporte de cobre telefónico. El ordenador está conectado a este módem por un cable de par trenzado, con conectores RJ45 o por cable USB. Desde el punto de vista del software, se crea en el ordenador una configuración *Point to Point over Ethernet* (PPoE), que permite la conexión hasta el Proveedor de Acceso a Internet (PAI) o *Internet Service Provider*(ISP).

b. Los diferentes servicios

La primera solución comercial que se ofreció fue ADSL. Se definió en 1995 y ofrecía la utilización de un canal telefónico analógico o RDSI. Las velocidades previstan eran de:

- 800 Kbps máximo de velocidad de subida (desde el abonado a la central).
- 8,192 Mbps máximo de velocidad de bajada (desde la central al abonado).

Gracias a los avances tecnológicos, hoy en día se puede llegar a:

- 1.024 Kbps de subida.
- 28,672 Mbps de bajada.

Las tecnologías DSL dependen mucho de la distancia hasta la central. Por eso, la velocidad máxima ADSL no se alcanza al sobrepasar los 2,4 kilómetros de bucle local. La evolución*Reach Extended* ADSL prolonga esta distancia alrededor de 800 metros más.

Después de este primer tipo de ADSL, han surgido otros, como:

- *High bit rate DSL* (HDSL), simétrica a 2 Mbps como máximo a unos 3,6 kilómetros.
- *Symmetric DSL* (SDSL), a 2 Mbps como máximo para distancias de unos 2.400 metros, pero con tiempos de espera muy convincentes.
- *Single-pair High-speed DSL* (SHDSL), de 144 Kbps a 2,3 Mbps, hasta 5.400 metros, pero con una velocidad fija garantizada (importante para las videoconferencias).
- *Very high speed DSL* (VDSL), capaz de picos de bajada de hasta 100 Mbps, pero a 300 m de la central como distancia máxima (por encima, similar al ADSL 2+ presentada anteriormente, pero para 3.500 metros).

Dirigida principalmente a particulares, la ADSL ha evolucionado y hoy muchos proveedores de conexión ofrecen a sus clientes el uso de la tecnología ADSL 2+, que puede alcanzar picos de 20 Mbps, pero a 2,5 kilómetros como máximo. Para distancias mayores, está el ADSL clásico. En los extremos, tanto el módem como el DSLAM se han tenido que adaptar al ADSL 2+.

Cada vez con más frecuencia, los ISP ofrecen velocidades en ATM, la que se da entre la red Internet y el DSLAM del ISP. La velocidad real es la IP, alrededor de un 25 % más lenta.

En España, sobre todo gracias a estas tecnologías xDSL, el acceso a Internet a alta velocidad se ha convertido en una realidad. Las comunicaciones son ahora tan fiables y rápidas que un gran número de empresas abandonan las costosas líneas dedicadas para contratar redes privadas virtuales (VPN - *Virtual Private Network*) permanentes, controladas por la empresa. Para ello, basta con configurar dos routers, que crearán un túnel seguro a través de Internet, sin otro compromiso con los operadores que la contratación necesaria.

c. Las ofertas «Triple play»

Con el acceso desglosado total y el aumento de la velocidad en ADSL 2+, los proveedores de acceso a Internet han comenzado a hacer ofertas que van mucho más allá del simple acceso a Internet de alta velocidad.

Esta ofertas, denominadas «Triple play», incluyen:

- acceso a Internet de alta velocidad;
- tarifa plana telefónica, sobre IP (VoIP);
- televisión, con una amplia gama de canales de pago.

Estas ofertas solo están disponibles para los abonados más próximos a los DSLAM.

La interfaz entre la toma telefónica y los distintos dispositivos (televisión, ordenador, teléfono...) se hace con módems especiales adaptados para «Triple play». Los contectores que se utilizan son RJ11, RJ45 y SCART.

En España, los diferentes ISP llaman a estos dispositivos «box». A veces existe la posibilidad de un cuarto servicio: la conexión del teléfono móvil mediante Wi-Fi a la conexión de Internet del hogar para llamar por teléfono con este dispositivo sin pasar por la red GSM.

5. Cable público

Algunos núcleos urbanos ofrecen una solución alternativa de acceso a Internet, a través del cable de fibra óptica. Al contrario que en las tecnologías DSL, hay que conectar a los abonados a la arquitectura de red de fibra óptica a medida que se den de alta.

España ha dado poco apoyo a este soporte, muy costoso de instalar. La competencia de las tecnologías DSL, que se basan en una red que cubre ya todo el territorio, ha tenido mucha influencia. Por el contrario, empiezan a verse los límites de las tecnologías DSL, y el cable, que ofrece velocidades mucho mejores, aún tiene futuro. Por el momento, solo está disponible en núcleos urbanos muy grandes.

Las ofertas propuestas por los operadores de cable son muy similares a las del ADSL, con velocidades actualmente equivalentes e incluso superiores. Estos operadores también ofrecen «Triple play».

6. WiMax

a. El bucle local inalámbrico

Las soluciones de acceso a Internet de alta velocidad DSL utilizan las líneas RTC. Desgraciadamente, estas tecnologías no pueden cubrir toda la población, y no permiten el acceso de alta velocidad a Internet a todo el mundo. Hay que tener en cuenta que el cableado de fibra óptica se reserva a núcleos urbanos cuya densidad de población sea muy alta.

La utilización de la solución Bucle Local Inalámbrico (BLI) permite evitar esta problemática. BLI se convierte así en una solución complementaria a las tecnologías xDSL y al cable público, que permite a los entornos profesionales y a los hogares acceder a Internet a alta velocidad.

Mediante las autorizaciones adecuadas, otros operadores alternativos a Telefónica puede crear sus propias redes BLI.

Para los proveedores de acceso a Internet, la BLI es una solución a algunos problemas de acceso desglosado. De hecho, para estos operadores es muy difícil reproducir una red de telecomunicaciones completa que llegue al cliente final. En ofertas de acceso desglosado parciales, el operador alternativo conecta el bucle local, que pertenece a Telefónica, con su propia red. Para esto, coloca sus equipos de transmisión en los locales del operador principal, del cual es competidor. La desagrupación total implica, además, que el ISP alquile la línea de bucle local. Por ello es comprensible que la utilización de BLI permita simplificar algunas operaciones.

b. Las solución WiMax

El grupo de trabajo IEEE 802.16 *Broadband Wireless Access Working Group* (BWAWG) estandariza las soluciones de tipo RMAN utilizables por BLI. Para promoverlas, Intel y Alvarion crearon en 2002 una asociación, la *Worldwide Interoperability Microwave Access*(WiMax) *forum*. Actualmente, esta agrupación cuenta con numerosas empresas asociadas.

Además de la promoción de esta tecnología, el objetivo de esta asociación es facilitar la

certificación de hardware para garantizar su compatibilidad.



El logo WiMax

El estándar IEEE 802.16a, ratificado en enero de 2003, sirvió de base a WiMax. Permite velocidades simétricas que teóricamente llegan a los 70 Mbps, dentro de un alcance cercano a los 50 kilómetros. En realidad, los operadores hablan de una velocidad real máxima de 12 Mbps para un alcance de 10 a 20 kilómetros, en función del entorno.

Algunas antenas de infraestructura pueden bastar para poner en marcha una conexión punto a multipuntos a nivel de una comarca. Este primer estándar, que solo regula la conexión fija, evolucionó levemente al 802.16d, también llamado 802.16-2004, ratificado en junio de 2004.

La evolución 802.16e, aprobada en diciembre de 2005, trae la movilidad a WiMax. Prevé el paso de una antena a otra (*Hand-over*) y el desplazamiento a bordo de un vehículo sin interferencias en la comunicación. Su velocidad teórica es de 30 Mbps y su alcance es de 3,5 kilómetros. Para comunicarse, los ordenadores portátiles y otros equipos móviles han de tener integrado un componente dedicado.

La nueva versión 2 de WiMax está a punto de finalizarse (IEEE 802.16m).

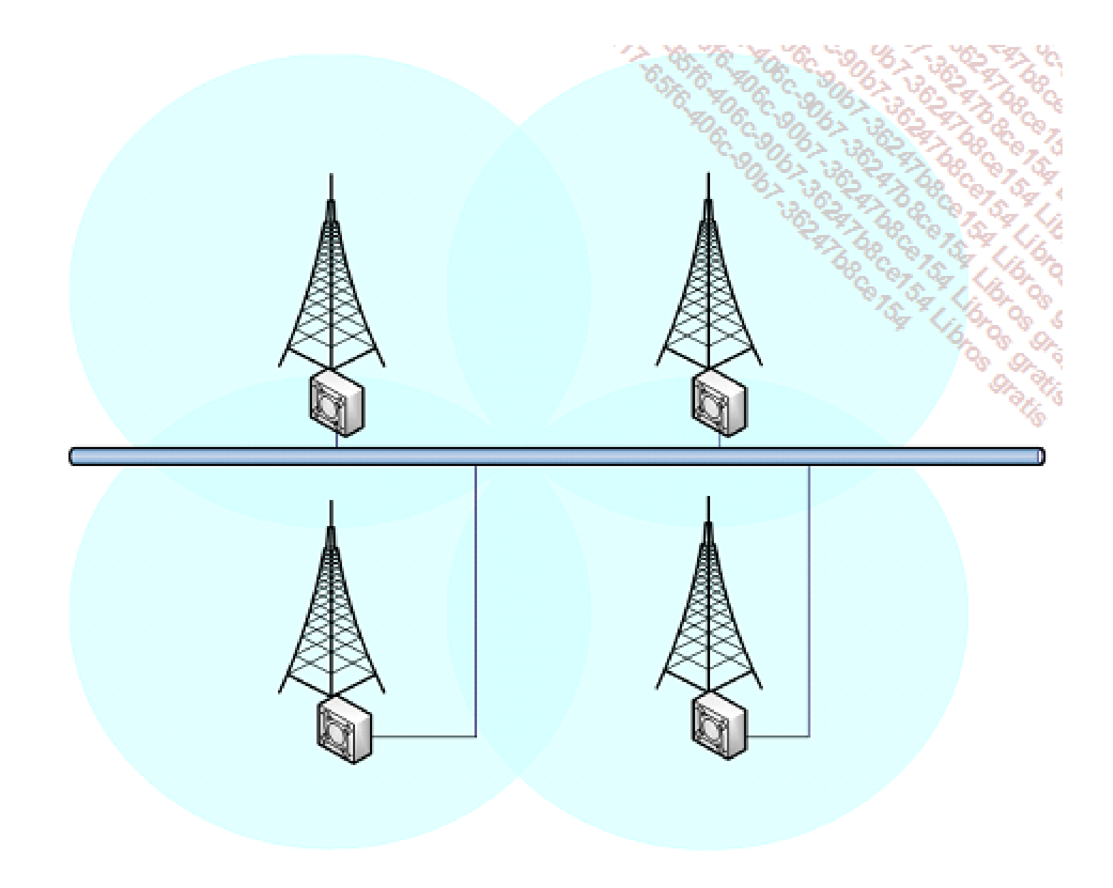
Esta versión permite velocidades teóricas de 1 Gbps. Este estándar debe permitir la convergencia de las tecnologías Wi-Fi, WiMax y 4G.

7. Redes móviles

a. Inicios

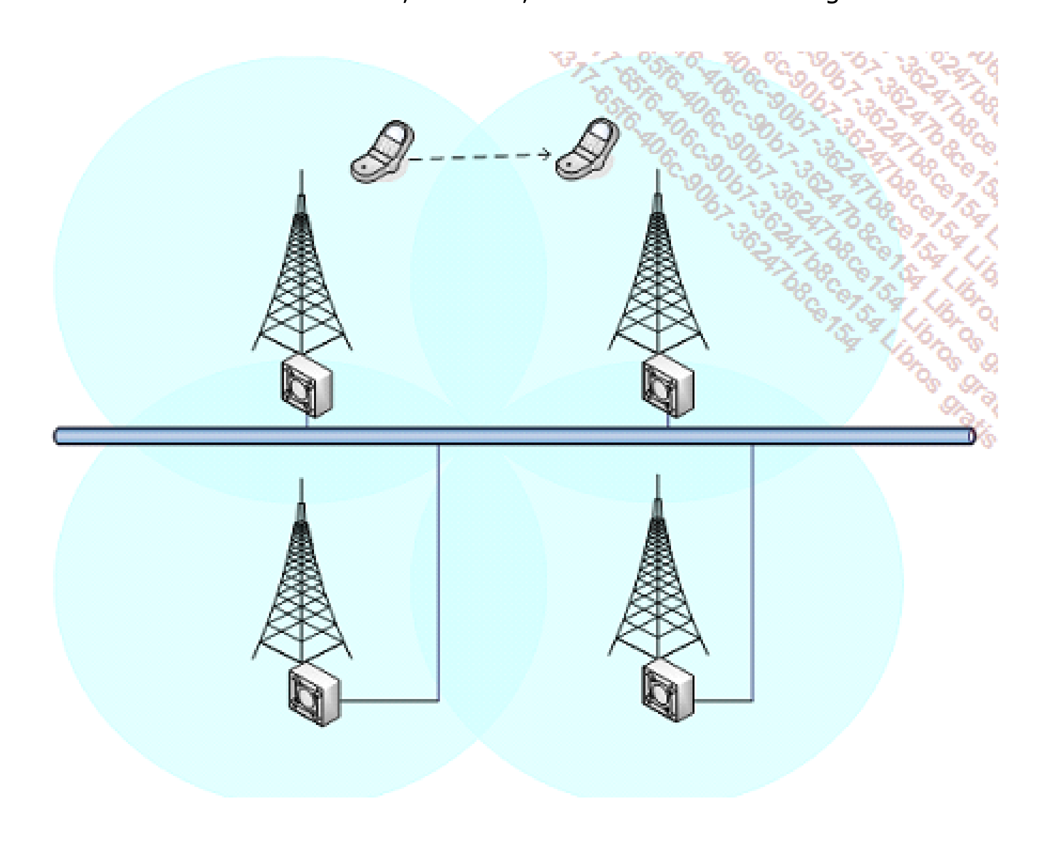
Hace ya algunos años, la telefonía móvil invadió nuestra vida diaria. También en este ámbito, la convergencia de las redes de voz y datos está de actualidad.

En estas redes, una antena (RAN - *Radio Access Network*) cubre una determinada zona geográfica. Todos los puntos que pueden alcanzarse a partir de este equipo forman una celda. Una estación de base, vinculada a la antena, desempeña el papel de servidor para todos los clientes de la celda. Una red central (CN - *Core Network*) conecta entre sí las distintas estaciones básicas.



Esta organización en celdas geográficas permite la transferencia de datos entre ellas durante la comunicación. De hecho, el equipo móvil verifica continuamente la calidad de las señales recibidas. Si su estación de base no le proporciona la mejor señal posible, pide un cambio al administrador de la red central. Esta acción de comunicación tiene el nombre de *hand-over*,*handover* o *handoff*. En telefonía móvil, la capacidad de *roaming*, o itinerancia, implica un acuerdo entre operadores para acceder a su red desde el extranjero.

Estos conceptos y denominaciones se pueden encontrar en redes de tamaño inferior, RMAN o RLAN. El término *hand-over* indica también, a veces, un cambio de tecnología.



b. El comienzo

A finales de los años setenta, la red Radiocom 2000 se convirtió en la primera generación (1G) de telefonía móvil. El funcionamiento era completamente analógico, con conmutación de circuito. La red estaba formada por celdas de algunos kilómetros de alcance.

A principios de los años ochenta, la Conferencia Europea de correos y Telecomunicaciones (CEPT) empezó a estandarizar un sistema digital de telefonía móvil. Y para ello reservó las bandas de frecuencias cercanas a los 900 MHz. En 1987, el grupo de estudio GSM, Grupo Especial Móvil, del CEPT lanza el sistema de telefonía *Global System for Mobile* (GSM). En esta segunda generación (2G), el transporte es digital y optimizado para la voz.

La evolución de este último, que utiliza la banda de 1800 MHz, el *Digital Cellular* (DCS 1800), se establece rápidamente en 1990.

No hay ninguna razón técnica que se oponga a esta evolución y se intenta un primer servicio de datos a través de GSM: *Wireless Application Protocol* (WAP). Los datos se modulan con la señal de voz para reconstruirse a continuación por demodulación. Su velocidad es de 9,6 Kbps.

c. La evolución hacia el transporte de datos

La solución WAP, que fue un fracaso comercial, encontró un sucesor con *General Packet Radio Service* (GPRS), al que a veces se denomina como generación 2.5. Se trata de una verdadera adaptación de las redes móviles a la transferencia de datos. La conexión puede ser permanente, puesto que utiliza la técnica de conmutación de paquetes. En los terminales, GSM es quien administra las transferencias de voz (la facturación depende del tiempo de comunicación), mientras que GPRS administra la transferencia de datos (la facturación depende del volumen de datos transferidos).

Esta nueva tecnología permite una velocidad teórica que llega hasta los 115 Kbps, realmente 40 Kbps, adaptando su velocidad a la calidad de la red. Gracias a ella, las PDA pueden comunicarse realmente y han aparecido otras soluciones.





Terminales móviles utilizables para datos

GPRS evoluciona a EDGE (*Enhanced Data for GSM Evolution*), tecnología igualmente dedicada a la transferencia de datos en paquetes. Reutiliza las infraestructuras de las redes GSM existentes y permite aumentar la velocidad de transferencia. Puede alcanzar una velocidad de 384 Kbps. EDGE se considera como una solución intermedia entre GPRS y UMTS y se le llama la generación 2.75.

Pero, a pesar de todo, estas velocidades siguen siendo insuficientes y es difícil ofrecer aplicaciones multimedia con GPRS o EDGE, como por ejemplo la televisión o la videotelefonía. Además, a escala mundial, los distintos sistemas de comunicación móvil 2G son incompatibles. La Union Internacional de las Telecomunicaciones (UIT) propuso en 1985 la definición del programa *Future Public Land Mobile Telecommunications System* (FPLMTS) para utilizar una banda de frecuencias única y ofrecer accesos de hasta 2 Mbps.

El conjunto de especificaciones de este programa, finalmente bautizado como sistema*International Mobile Telecommunication 2000* (IMT 2000), llamó la atención del ETSI, que propuso su solución como respuesta: *Universal Mobile Telecommunications System* (UMTS). Otros organismos se agruparon en torno a esta solución para formar el consorcio *3rd Generation Partnership Project* (3GPP), que adopta UMTS a nivel mundial a principios de 1998. EE. UU. finalmente adoptar el sistema CDMA2000, resultado de los trabajos del grupo 3GPP2.

d. Las nuevas generaciones de telefonía móvil

En Europa, UMTS se convierte en la 3.ª generación (3G) de telefonía móvil.

Se establece una velocidad máxima de 384 Kbps de recepción para contrarrestar las grandes dificultades del *hand-over*. Ahora es posible la transferencia de datos entre dos móviles a la velocidad de un automóvil. Además, es posible intercambiar datos entre 2G y 3G sin pérdida de información.

La inversión necesaria por parte de los operadores de telefonía móvil para pasar a UMTS es importante. Las velocidades siguen siendo muy limitadas para aplicaciones que permitan recuperar la inversión. Rápidamente el UTMS evolucionó a HSDPA (*High Speed Downlink Packet Access*), considerado como el ADSL para la telefonía móvil. Esta generación 3G+ permite velocidades de más de 7 Mbps.



Tarjetas módem 3G o 3G+ en formato PCCard o USB

La futura revolución de las redes inalámbricas podría ser la utilización del estándar de comunicación *Unlicensed Mobile Access* (UMA). Permitirá el *roaming* entre redes 2G o 3G a Wi-Fi o Bluetooth, sin cortes de comunicación. Esta solución, llamada *Intelligent Transportation Systems* (ITS), podría hacer necesaria la utilización de una dirección IP fija.

La 4G o cuarta generación hace referencia a un conjunto de criterios, tanto de velocidad como de calidad del servicio. Esta generación se conoce también como *Long Term Evolution* (LTE). Gracias a la utilización de múltiples conexiones de radio simultáneas, se puede incrementar la velocidad sustancialmente. Además, una menor latencia permite mejorar considerablemente la implementación de aplicaciones en tiempo real.

De hecho, mientras que las velocidades teóricas de 3G+ tienen un tope de 42 Mbps (7 Mbps en la práctica), la LTE anuncia velocidades teóricas de 100 Mbps de descarga y 50 Mbps de subida.

Para muchos operadores, el desarrollo de *smartphones* ha generado un tráfico de datos que se ha disparado en los dos últimos años. Algunas grandes ciudades tienen problemas de saturación en horas punta.

Después del lanzamiento, por parte de TeliaSonera, de la primera red operativa en Suecia en septiembre de 2009, Ericsson ha desplegado la alta velocidad móvil y MetroPCS la opera en EE. UU. (Dallas y Fort Worth, en Texas).

En junio de 2011, la CMT (Comisión del Mercado de las Telecomunicaciones) ha asignado en concurso las licencias 4G LTE (*Long Term Evolution Advanced*). Orange se ha hecho con las frecuencias de los 900 MHz por 443 millones de euros y ha obtenido 10 MHz.

Yoigo ha obtenido 30 MHz de las frecuencias de los 1800 MHz por 300 millones de euros. Telefónica ha adquirido 20 MHz en la banda de 800 MHz, 10 MHz en la banda de 900 MHz y 40 MHz de la banda de 2,6 GHz por un toal de 668 millones de euros. La segunda fase de concesión de licencias es en 2015.

Samsung ha sido uno de los primeros en implementar 4G en sus *smartphones*:



Smartphone 4G

Del mismo modo, se comercializan llaves USB para permitir la conexión desde ordenadores portátiles:



Llave 4G

8. Fiber Distributed Data Interface (FDDI)

Esta tecnología de red metropolitana (MAN) fue desarrollada por los pioneros de la Sperry Corporation en 1982. Fue propuesta a ANSI, y después estandarizada por ISO con el número 9314. Es compatible con LLC e incluye una capa inferior MAC.

a. Principios

FDDI define una comunicación en un anillo doble con testigo contrarrotatorio, uno para cada sentido.

Originalmente, la velocidad es de 2*100 Mbps, a través de una fibra óptica monomodo o multimodo. Esta velocidad aumentó a 2*155 Mbps en FDDI-2, luego a 2*2,5 Gbps con la evolución *FDDI Follow On LAN* (FFOL).

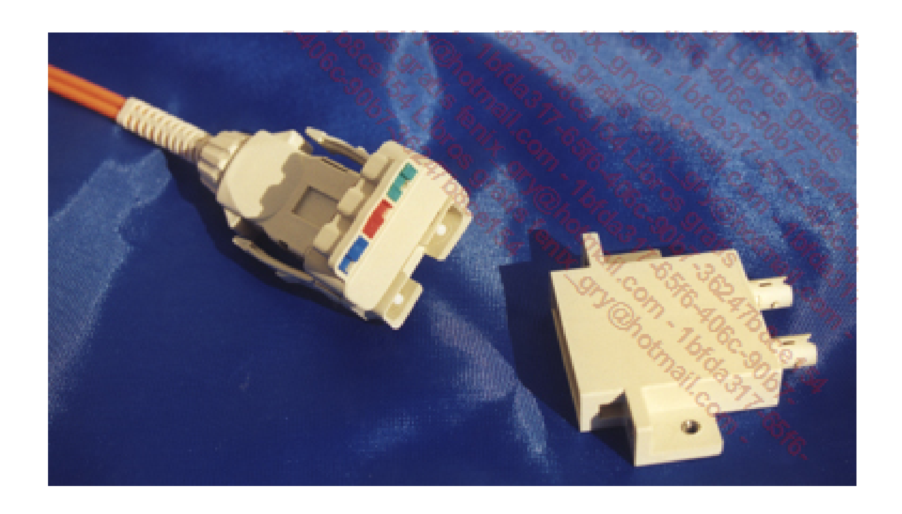
FDDI 2 funciona de manera síncrona, lo que permite transmisiones multimedia y transmisión de voz.

Hay alternativas que utilizan el par trenzado, como la *Copper Distributed Date Interface* (CDDI).

La distancia máxima entre dos conexiones es de 2 km con una fibra multimodo y de 60 km con una fibra monomodo.

b. Topología

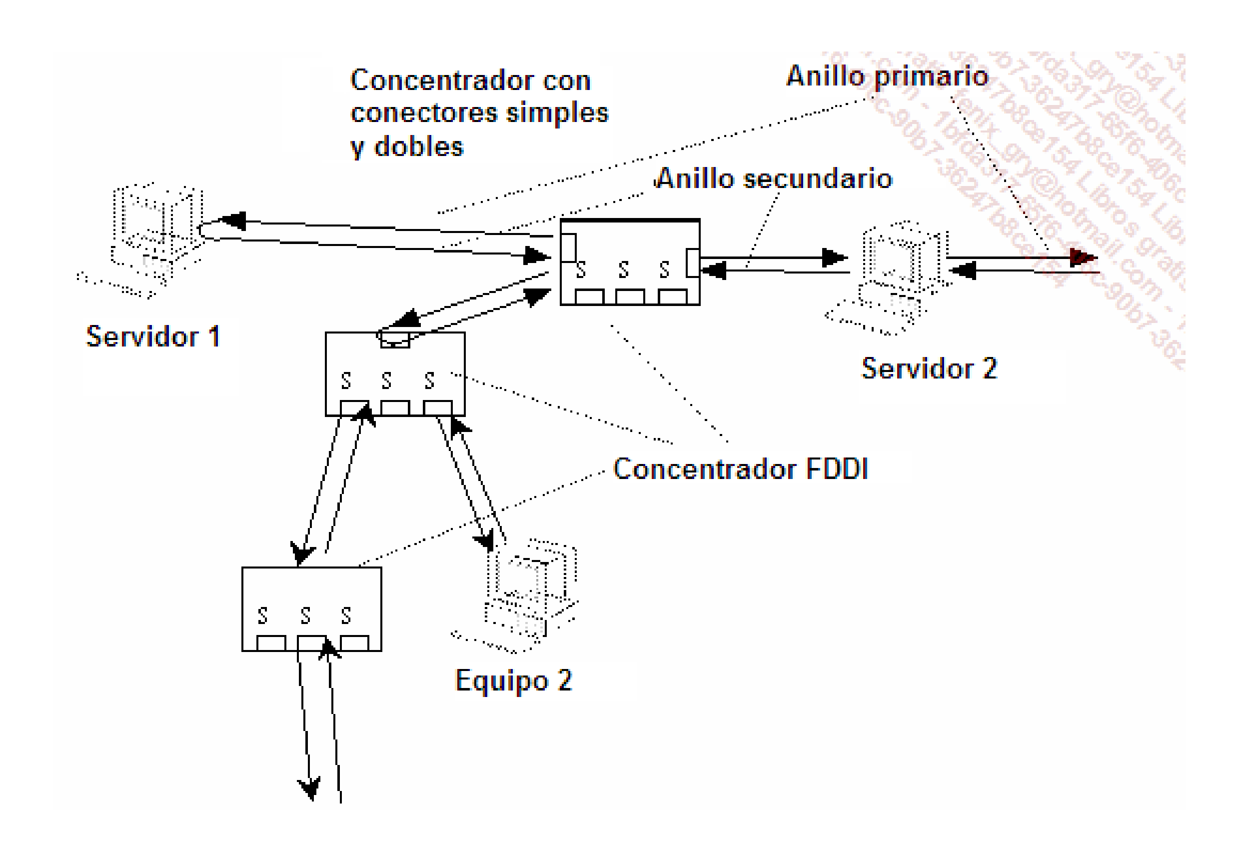
La red FDDI puede conectarse directamente al ordenador o a un *hub*.



Conectores FDDI

Se pueden utilizar diferentes métodos de conexión, con diferentes tipos de conector:

- A, doble conexión en cada anillo.
- B, doble conexión en un único anillo.
- C, concentrador conectado al doble anillo para conectar las estaciones B.



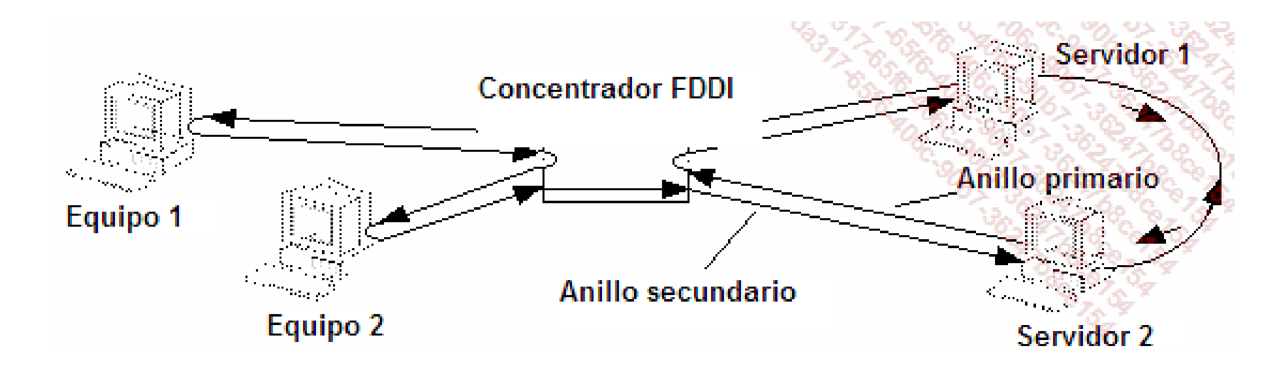
Conexión FDDI en árbol con tolerancia a fallos

c. Funcionamiento

FDDI está calculada para redes de tipo MAN, pero puede ser utilizada como medio de interconexión entre LAN (troncales). El LLC utiliza sus servicios y su tecnología es cercana al 802.5.

Mejora el paso de testigo. En cuanto se emite el testigo, se produce una disminución de carga que permite repetir las tramas de equipo en equipo y poner al testigo en última posición para que las máquinas lo puedan registrar. De esta manera, agregan sobre el testigo su propia información, que irá al final de cada ciclo de tramas.

La arquitectura de dos anillos con sentidos contrarios de circulación permite retomar el ciclo automáticamente en caso de fallo, y de esta manera se garantiza una fuerte tolerancia a fallos en los equipos.



En FDDI es posible disponer de 500 estaciones en un anillo de 100 km de perímetro. Cuando cada estación participa de la tolerancia a fallos en caso de corte, el reinicio del ciclo aumenta el tamaño total del anillo a cerca de 200 km y a 1000 máquinas.

Cada equipo se comporta como un repetidor, función que es necesaria cada 2 km.

Después de una vuelta al anillo, una trama puede presentar distintos estados que permitirán a su emisor saber si la recibieron correctamente. El estado inalterado indica que el destinatario no vio pasar la trama. En cualquier otro caso, el receptor modifica la trama para indicar que la copió o que

la rechazó, debido a un error de CRC o por falta de espacio en el *buffer* de recepción del destinatario de la trama.

La codificación completa es de tipo NRZI - 4B / 5T.

9. Asynchronous Transfer Mode (ATM)

ATM nació de la fusión de la telefonía y la informática. El ATM Forum mantiene esta tecnología desde 1991.

a. Principios

ATM debía permitir la transmisión de voz, vídeo y datos en redes de gran tamaño y a grandes velocidades. Para ello fue necesario adoptar un método que permitiera una velocidad no variable (asincronismo) para los flujos multimedia.

Se implementó una conmutación de paquetes de tamaño fijo y reducido, las celdas. Esta conmutación de celdas permite velocidades de 155 Mbps, 622 Mbps o más. Se acopla con una clase de conmutación de nivel físico por instauración de circuitos virtuales multiplexados.

ATM se utiliza tanto como troncal en redes de tamaño relativamente pequeño como en las redes WAN.

b. El enlace de celdas

ATM es una forma de enlace de celdas (*Cell relay*). Una celda ATM es una trama fija, de 53 bytes, de los cuales 48 son de datos.

Este valor es una prueba de isocronismo para el muestreo. Como hemos visto anteriormente, se prevé que la digitalización de la voz contenga un byte cada 125 microsegundos. Se necesitan 6 milésimas tanto para completar como para vaciar una celda del receptor. Entre estas dos acciones, el transporte no debe excederse demasiado en el tiempo.

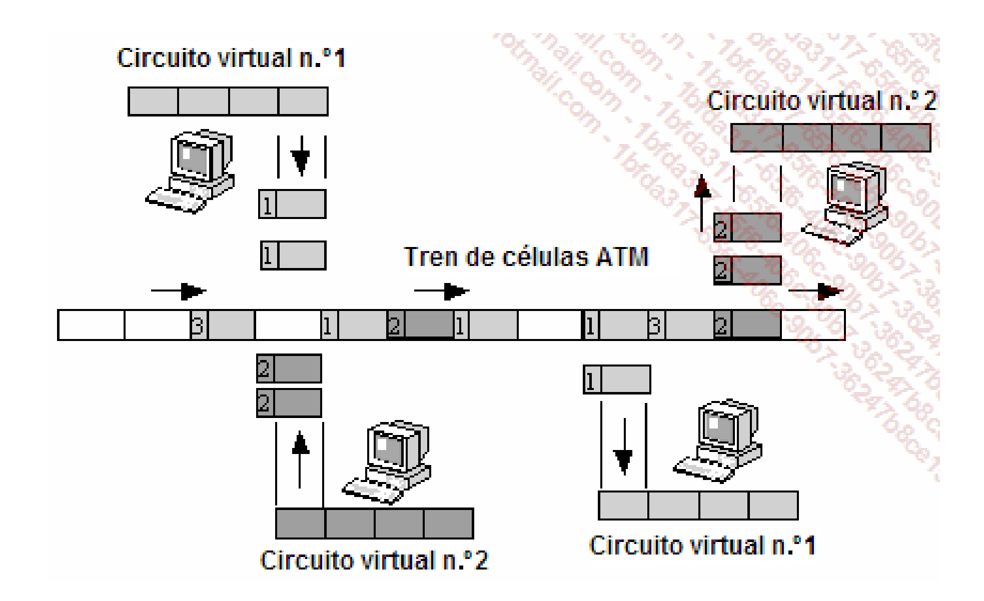
En una red ATM, cada equipo emite continuamente, aunque las celdas estén desocupadas. Esta tecnología también tiene en cuenta los soportes de comunicación, los considera como una clase de memoria física durante el enrutamiento de las celdas.

Las celdas son de dos tipos y sus encabezados son diferentes:

- *Network Node Interface* (NNI), entre dos nodos de red.
- *User Network Interface* (UNI), para la entrada y salida de la red.

c. Regulación del tráfico

El protocolo ATM integra una asignación dinámica del ancho de banda, gracias a un multiplexado temporal asíncrono.



Gracias a este multiplexado, la conexión se efectúa a dos niveles. Las vías virtuales (VCI -*Virtual Channel Identifier*) son dos secciones identificadas por un número constante de VCI. En el interior de estas vías, los caminos virtuales (VPI - *Virtual Path Identifier*) aseguran las conexiones estáticas semipermanentes.

Las conmutaciones se realizan a dos niveles:

- En los paneles de conexión, cuya única función es la conmutación de señales.
- En los conmutadores, que actúan sobre VCI y los VPI.

Una celda de supervisión permite el establecimiento del circuito virtual. Utiliza una tabla de enrutamiento y determina la relación entre las vías de entrada y salida para cada nodo. Las relaciones se resumen en una tabla de conmutación.

d. Tipos de servicios

Con ATM se han definido cuatro clases:

- A, emulación de circuito de velocidad constante y flujo isócrono.
- B, emulación de circuito de velocidad variable y flujo isócrono.
- C, emulación de paquetes con conexión.
- D, emulación de paquetes sin conexión.

Los servicios que se asocian a estas clases:

- *Constant Bit Rate* (CBR), para voz y vídeo no comprimidos.
- *Variable Bit Rate* (VBR), para voz y vídeo comprimidos.
- *Available Bit Rate* (ABR), para la transmisión de datos e interconexión de redes locales.
- *Unspecified Bit Rate* (UBR), para la transmisión de datos.

Los tres primeros servicios implican parámetros de calidad de servicio y tipo de tráfico.

e. Topología y velocidades

La tecnología ATM abarca casi por completo desde la capa 1 a la 3 del modelo OSI.

El nivel físico, que se encarga de adaptar las celdas al soporte, se divide en dos partes:

- *Transmission Convergence* (TC) se encarga de la implementación.

- *Physical Medium* (PM) transmite en la red física.

Se definen tres modos de funcionamiento en la red física:

- *Plesiochronous Digital Hierarchy* (PDH), que utiliza las infraestructuras existentes.
- *Synchronous Digital Hierarchy* (SDH), que a largo plazo debería ser el único que se utilice.
- Celdas, para las redes privadas, en las que estas se pueden transmitir directamente sobre el soporte de transmisión.

A nivel de Conexión de datos, la propia capa ATM se encarga del transporte de las celdas de extremo a extremo, con la conmutación y el multiplexado necesarios. Soluciona los problemas de congestión, controla el flujo y adapta, si es preciso, la velocidad, insertando o eliminando celdas vacías. ATM es capaz de implementar la calidad del servicio.

Además, *ATM Adaptation Layer* (AAL) hace la conexión entre ATM y las capas superiores. Se divide en:

- *Segmentation And Reassembly* (SAR).
- *Convergence Sublayer* (CS).

AAL gestiona la segmentación y el montaje de la información, así como el tratamiento de errores y la recuperacion de la señal del reloj.

Las velocidades son las descritas en el apartado de las líneas dedicadas, que pueden utilizar ATM, como las tecnologías DSL. Entre ellas podemos encontrar las velocidades europeas E1, E2, E3 y E4. Las redes ATM de velocidades muy altas utilizan el modo de funcionamiento SDH.

10. Synchronous Optical Network (SONET) y Synchronous Digital Hierarchy (SDH)

a. Antecedentes

Desde sus comienzos, la transmisión telefónica de voz ha sufrido dos dificultades importantes:

- Un elevado número de comunicaciones simultáneas deben transitar por un mismo soporte físico.
- La interconexión de líneas entre grandes operadores debe soportar grandes diferencias de velocidad.

En los años setenta se utilizaba una tecnología llamada *Plesiochronous Digital Hierarchy* (PDH), que tuvo que evolucionar para poder cumplir con las crecientes demandas de transferencia. Progresivamente, fueron surgiendo otras necesidades. Para responder a estas demandas, los operadores tuvieron que adaptar sus ofertas, sobre todo en cuanto a la flexibilidad.

Para responder a esta problemática nacieron nuevos enfoques, *Synchronous Optical Network*(SONET) en Europa y *Synchronous Digital Hierarchy* (SDH) en EE. UU.



b. Las características de SDH

Las ventajas de SDH con respecto a PDH son importantes:

- Facilidad de inserción de una trama en el interior de un multiplex.
- Velocidades elevadas que se reservan para el mantenimiento y el seguimiento del grupo.

- Posibilidad de evolucionar alcanzando altas velocidades (la limitación es solo técnica).
- Arquitectura de red mejor adaptada a la seguridad de las comunicaciones.
- Mayor modularidad de los equipos.

Desde mediados de los años ochenta, se emprendieron numerosos trabajos para permitir que los operadores de telecomunicaciones pudieran hacer evolucionar sus infraestructuras de red óptica.

Finalmente, en 1988 se llegó a acuerdos internacionales que permitieron coincidir en una serie de recomendaciones para el SDH:

- G. 707: velocidad binaria de SDH.
- G. 708: interfaz de nodo de red para SDH.
- G. 709: estructura de multiplexado síncrona.

Luego se añadieron otras normas para enriquecer el SDH.

c. Velocidades

Con SONET, los niveles se clasifican en *Optical Contener* (OC). Algunos ejemplos de velocidades son:

- OC-1, a 51,84 Mbps.
- OC-3, a 155,52 Mbps.
- OC-9, a 466,65 Mbps.
- OC-24, a 1,244 Gbps.
- OC-48, a 2,488 Gbps.

Las velocidades SDH se codifican como *Synchronous Transport Module* (STM):

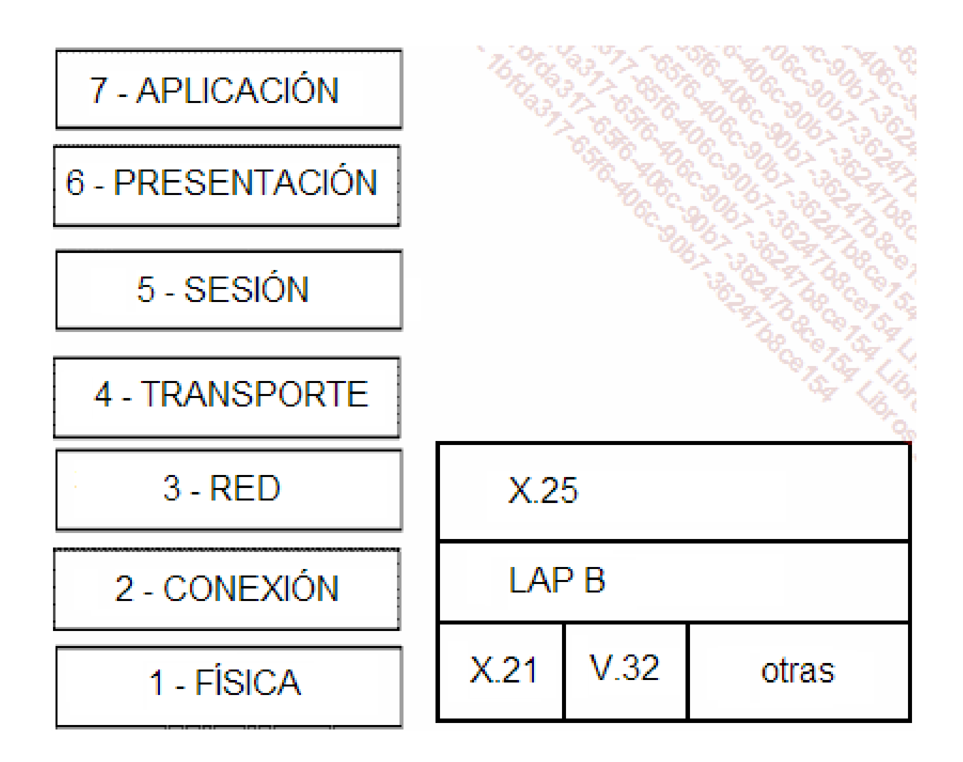
- STM-1, a 155,52 Mbps.
- STM-3, a 466,65 Mbps.
- STM-8, a 1,244 Gbps.
- STM-16, a 2,488 Gbps...

La velocidad OC-3/STM-3, cercana a 155 Mbps, a menudo se relaciona con ATM.

11. X.25

La especificación X.25 del CCITT data de 1974. Originalmente, se trataba de conectar terminales distantes con grandes sistemas, para lo que se utilizaba la RTC, pero resultó poco fiable.

Previa al modelo OSI, esta especificación describe un conjunto de protocolos integrados en una red de conmutación de paquetes por circuitos virtuales.



Comparación del modelo OSI y X.25

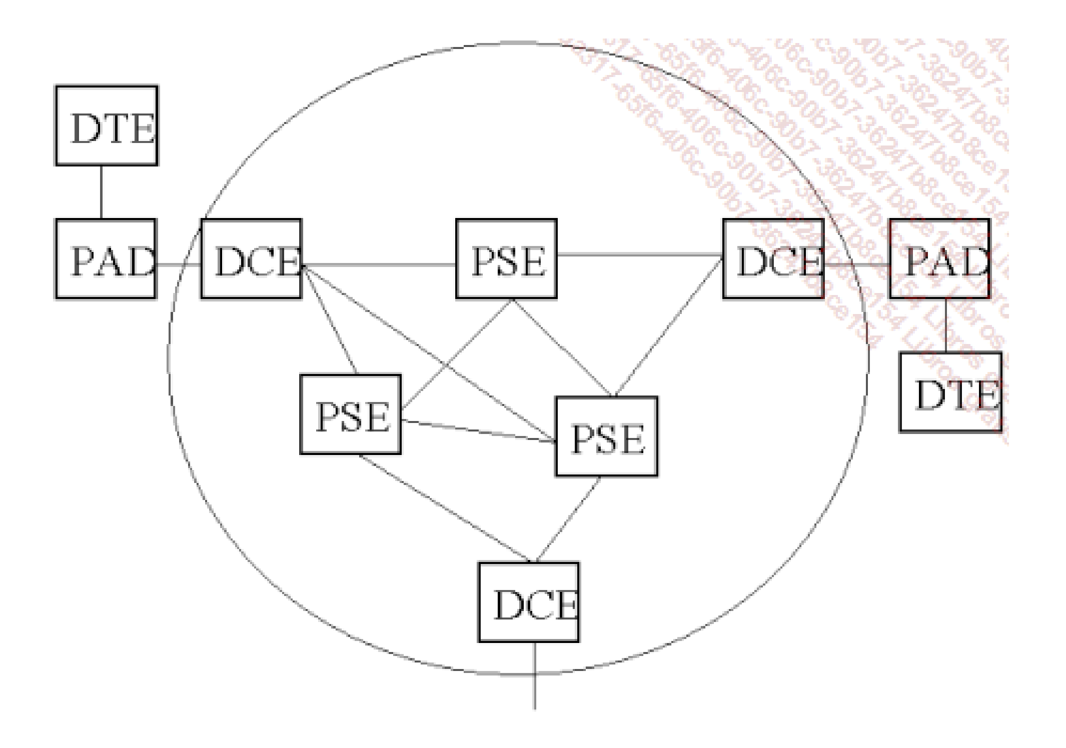
La especificación X.25 se extiende sobre las tres primeras capas del modelo OSI y se basa en el protocolo *Link Access Protocol B* (LAP B). Hay numerosos estándares disponibles para la capa física.

Asimismo, X.25 integra la identificación de paquetes y un reconocimiento de estos. Este protocolo administra, para cada circuito virtual, la recuperación de errores y el control de flujo. La arquitectura física de X.25 inicialmente fue pensada para la red telefónica existente, que no era muy fiable. Sin embargo esta corrección de errores asociada al control de flujo retrasa considerablemente X.25.

Sus velocidades no se adaptan a la conexión de una LAN. A pesar de todo, X.25 constituye una norma utilizada internacionalmente. Se desarrolla sobre todo en países que carecen de infraestructuras modernas.

En una red X.25, el equipo terminal (ETTD o DTE) se identifica con relación a ETCD o DCE. El conmutador se denomina *Packet Switching Exchange* (PSE).

El *Packet Assembler/Disassembler* (PAD) permite que un terminal no X.25 se conecte a la red, Iberpac en España. También es posible acceder a la red X.25 a través de la RTC (definida por la norma X.32).



Ejemplo de arquitectura X.25

Por ejemplo, Telefónica ofrece, con Iberpac, la conexión directa a X.25 cuyas velocidades fluctúan entre los 9,6 Kbps y los 1920 Kbps. Permite una conectividad universal con todos los abonados, así como con todos los usuarios de una red pública X.25 conectada al nodo de tránsito internacional.

También puede realizarse el acceso a través de la red telefónica conmutada, RTC, o de una conexión a la red digital de servicios integrados (RDSI).

12. Fr

Acceso remoto y redes privadas virtuales

El acceso a la red local de una ubicación desde el exterior, para el teletrabajo o para la interconexión entre dos sitios, por ejemplo, requiere la instalación de soluciones específicas.

Estos accesos remotos utilizan la modalidad punto a punto entre dos terminales localizables por medio de una dirección (como una IP pública) o un número de teléfono.

1. Utilización y evolución

Estos servicios se pueden clasificar en dos categorías.

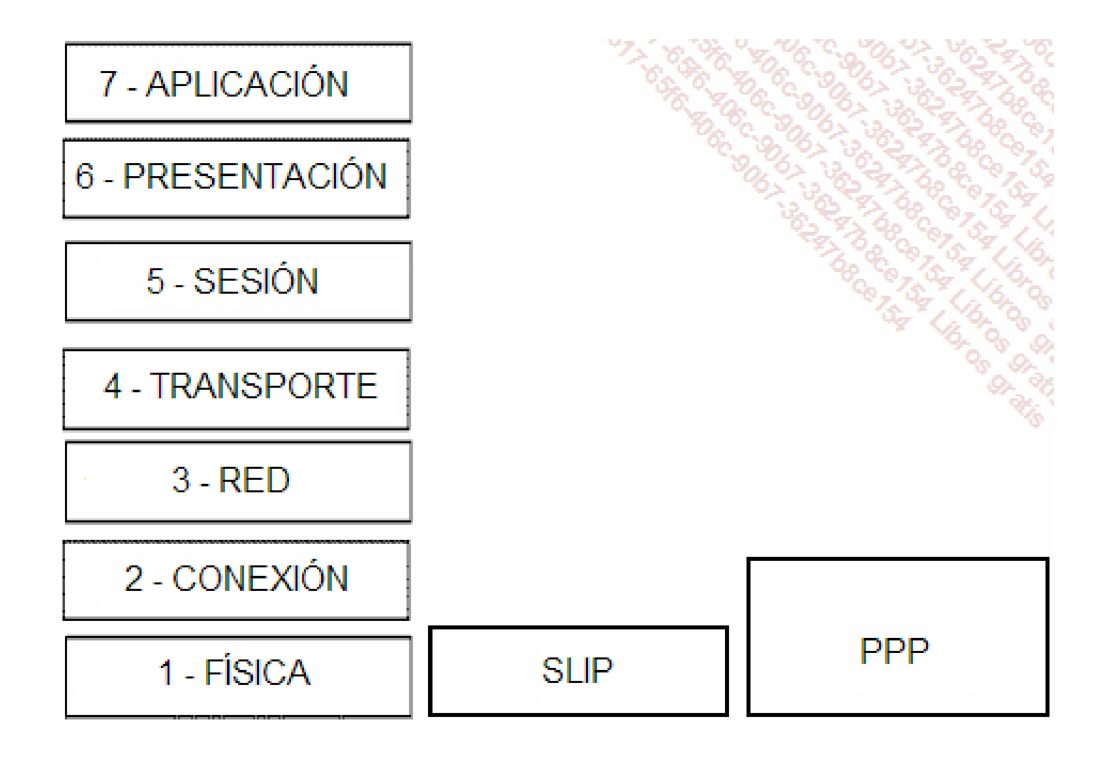
Si el acceso directo se realiza a través de un protocolo WAN, se habla de servicios de acceso remoto (RAS - *Remote Access Service*). A menudo se utiliza una solución por módem, con una facturación de la comunicación según tiempo y distancia.

Con la democratización de la conexión a Internet, las comunicaciones por acceso remoto con un módem analógico son poco comunes. Hoy en día lo normal es privatizar la comunicación en la red pública Internet. Para esto, se crea un túnel de aislamiento virtual y la comunicación cifrada se produce entre dos terminales, conectados a la red. Se habla de red privada virtual (RPV o VPN - *Virtual Private Network*).

La reducción de coste que implica la adopción de VPN ha generalizado su uso, tanto en la comunicación permanente entre lugares distantes como para accesos específicos de un puesto de trabajo en una empresa.

2. Protocolo de acceso remoto

El protocolo de nivel físico *Serial Line IP* (SLIP), que no era seguro, tiene su sucesor en el *Point to Point Protocol* (PPP) que cubre las dos capas bajas del modelo OSI.



Comparación de los modelos OSI, SLIP y PPP

PPP dispone de funcionalidades complementarias, como el control de errores y la seguridad. Soporta diferentes protocolos LAN de la capa de red.

3. Red privada virtual

Esta comunicación también es punto a punto entre un cliente y su servidor. El protocolo PPP se utiliza para el transporte.

a. Establecimiento de la conexión

Para poner en marcha la sesión VPN, en primer lugar se debe establecer una conexión a la red desde los dos extremos de la comunicación.



Tanto el cliente como el servidor deben soportar los diferentes protocolos que se utilizarán, a nivel de la comunicación, de la autentificación y del cifrado.

b. Autentificación

Cuando el cliente VPN pide acceso a su servidor, se exige, sobre todo, la autentificación del usuario.

La transferencia, la información de identificación y la contraseña se controlan de manera más o menos segura a través de una serie de protocolos estandarizados mediante PPP:

- *Password Authentication Protocol* (PAP) es poco recomendable, ya que la contraseña circula sin cifrarse.
- *Challenge Handshake Authentication Protocol* (CHAP) solo transmite una parte de la contraseña. Es un método más seguro que el anterior, pero aún es muy vulnerable en términos de seguridad.
- Microsoft CHAP versión 1 (MS-CHAPv1) y versión 2 (MS-CHAPv2) son versiones mejoradas de la anterior.

La verdadera confirmación de la seguridad llega con el mecanismo *Extensible Authentication Protocol* (EAP), que permite diferentes medios de autentificación, incluso el uso de un soporte físico o de la biometría.

c. El cifrado

Una vez que se supera la etapa de autentificación, se puede establecer el túnel de comunicación a distintos niveles del modelo OSI:

- Capa 2, con *Layer 2 Transport Protocol* (L2TP).
- Capa 3, *con Point To Point Tunneling Protocol* (PPTP) o *IP Security* (IPsec).
- Capas superiores con, por ejemplo, SSL/TLS.

Los dos protocolos PPTP y L2TP utilizan PPP para transportar los datos. L2TP reduce los encabezados, con una compresión de 4 bytes en lugar de 6.

El protocolo *Microsoft Point to Point Encryption* (MPPE) proporciona el cifrado en PPTP, utilizando el

algoritmo RC4. Se pueden utilizar contraseñas de 40, 56 o 128 bits. La autentificación, por ejemplo, se puede asegurar con MS-CHAPv1 o MS-CHAPv2. La solución PPTP/MPPE es la más antigua y tiende a utilizarse cada vez menos.

Si es necesaria la confidencialidad de la información transmitida por L2TP, el estándar de capa 3 IPsec garantiza la seguridad. Actualmente se recomienda la utilización de L2TP/IPsec para la realización de un túnel VPN en las capas 2 y 3.

Recientemente han aparecido nuevos tipos de red VPN. Considerando que todos los equipos de trabajo pueden interpretar las tramas SSL/TLS, por ejemplo gracias a los navegadores, la VPN-SSL favorece una solución sin despliegue ni instalación de cliente (*client less*). Además, el tráfico seguro por este método utiliza un puerto generalmente abierto en los cortafuegos, el TCP 443, correspondiente a HTTPS.

4. Clientes sencillos y acceso remoto

La banda ancha necesaria para las comunicaciones de acceso remoto o en una VPN se puede reducir por el uso de soluciones de tipo terminal, en las cuales el tráfico se reduce a:

- La transmisión de imágenes de pantalla en un sentido.
- La transmisión de las pulsaciones sobre el teclado y los movimientos del ratón.

Estas soluciones se utilizan también para redes locales, sobre las que aportan racionalización de los costes y facilidad de gestión.

Por ejemplo, un servidor Windows que incorpora la funcionalidad Servicios de escritorio remoto (RDS) puede unirse gracias al «Escritorio remoto», en lado del cliente, a través de una VPN o no. El protocolo de transmisión utilizado en las capas altas es *Remote Desktop Protocol* (RDP).

La empresa Citrix ofrece una solución similar con el servidor Xen App (p. ej., Presentation Server, el propio Metaframe). El protocolo que se utiliza es *Independent Computing Architecture*(ICA) y se debe instalar el cliente. El software de enlace *Citrix Secure Gateway* (CSG) se puede añadir en la empresa para una comunicación de terminal a través de una red privada virtual e Internet.

Existen también otras soluciones.

Principales familias de protocolos

Con la aparición de las redes locales, se utilizaron distintos protocolos de capas medias y altas, a menudo vinculados a un editor de programas. Con el tiempo se han ido sustituyendo por el estándar de hecho TCP/IP.

1. IPX/SPX

a. Antecedentes

Históricamente, se ha utilizado esta familia de protocolos con las redes Novell Netware hasta la versión 3.12. TCP/IP ya estaba disponible en esta versión, pero IPX/SPX era absolutamente necesario para asegurar el buen funcionamiento del sistema operativo, además de, en algunas ocasiones, el TCP/IP. Hoy en día casi nadie lo utiliza, incluso aunque a menudo esté configurado en las impresoras de red.

b. Protocolos

Internetwork Packet eXchange (IPX) actúa en las capas de red y transporte. Provee, como IP, un servicio sin conexión ni seguridad.

IPX es enrutable e identifica un equipo a través de una dirección lógica que no requiere, como IP, un plan de direccionamiento estático. Una dirección IPX es la concatenación de un número de red externo, en 4 bytes, y de la dirección MAC del dispositivo, en 6 bytes. La asignación de direcciones IPX es automática y, por añadidura, la resolución de direcciones lógicas en direcciones físicas es instantánea, ya que la dirección física forma parte de la dirección IPX.

Las direcciones IPX se presentan, por ejemplo, de la siguiente manera: 0000CAFE: 00-A0-00-26-37-10, donde 0000CAFE es el número de red lógica en hexadecimal en 4 bytes y 00-A0-00-26-37-10 es la dirección MAC de la tarjeta de red.

En Netware, no se debe confundir el número de red externo (vinculado a los dispositivos) con el número de red interno (vinculado a las aplicaciones). Este último está vinculado a la estructura interna de Novell que asocia las aplicaciones de un servidor a un número de nodo y un número de red. El servidor funciona entonces como un router interno que conmuta la red física (número de red externo) con la red lógica (las aplicaciones del servidor). Así pues, un servidor Novell posee dos direcciones de red, una dirección interna y otra externa.

Como para IP, todos los nodos conectados a la misma red física deben tener el mismo número de red (externo) y cada dirección IPX debe ser única en la red. Del mismo modo, los números de red internos utilizados deben ser únicos.

Una de las particularidades de IPX es la de poder provocar un cortocircuito en el modelo OSI, al dirigirse directamente a la capa 5 del destinatario y no forzosamente a SPX. Los protocolos IP + TCP corresponden a IPX + SPX, mientras que los protocolos IP + UDP corresponden únicamente a IPX.

Sequenced Packet eXchange (SPX) se aplica en la capa Transporte del modelo OSI y garantiza una entrega fiable de los paquetes (orientada a la conexión).

2. NetBIOS

a. Antecedentes

Network Basic Input/Output System (NetBIOS) fue introducido por IBM en 1985, quien lo optimizó para redes pequeñas. Su implementación es sencilla, pero no es enrutable. Introduce nombres

NetBIOS para identificar los puestos de la red, sin administrar direcciones lógicas. No existe más que una resolución de nombre en direcciones MAC. Además, es el propio equipo el que administra esta solución enviando una difusión a la red.

b. Principio

La simplicidad de este protocolo y el hecho de que consuma pocos recursos de memoria hace que NetBIOS todavía sea utilizado por los productos de Microsoft, IBM y Novell.

Las *Application Programming Interface* (API) NetBIOS se han desarrollado ampliamente para PC, para permitir una independencia del protocolo subyacente utilizado.

Las fuentes de NetBIOS están disponibles, encapsuladas en tramas LLC (802.2) o encapsuladas en IPX o en TCP/IP.

Muchos de los productos Microsoft todavía funcionan con NetBIOS. Sin embargo, se puede utilizar cualquier otro protocolo de capas 3 y 4, como TCP/IP, IPX/SPX o NetBEUI.

NetBIOS sigue estando presente en los sistemas operativos MS Windows, a través de NBT (*NetBIOS over TCP/IP*).

Hasta la llegada de Windows 2000, los sistemas operativos de Microsoft obligaban a utilizar NetBIOS, en particular por su popular servicio de archivos *Server Message Block* (SMB).



En las versiones Unix/Linux que implementan SaMBa (SMB rescrito por Andrew Tridgel), NetBIOS se instala automáticamente en forma de un demonio nmbd.

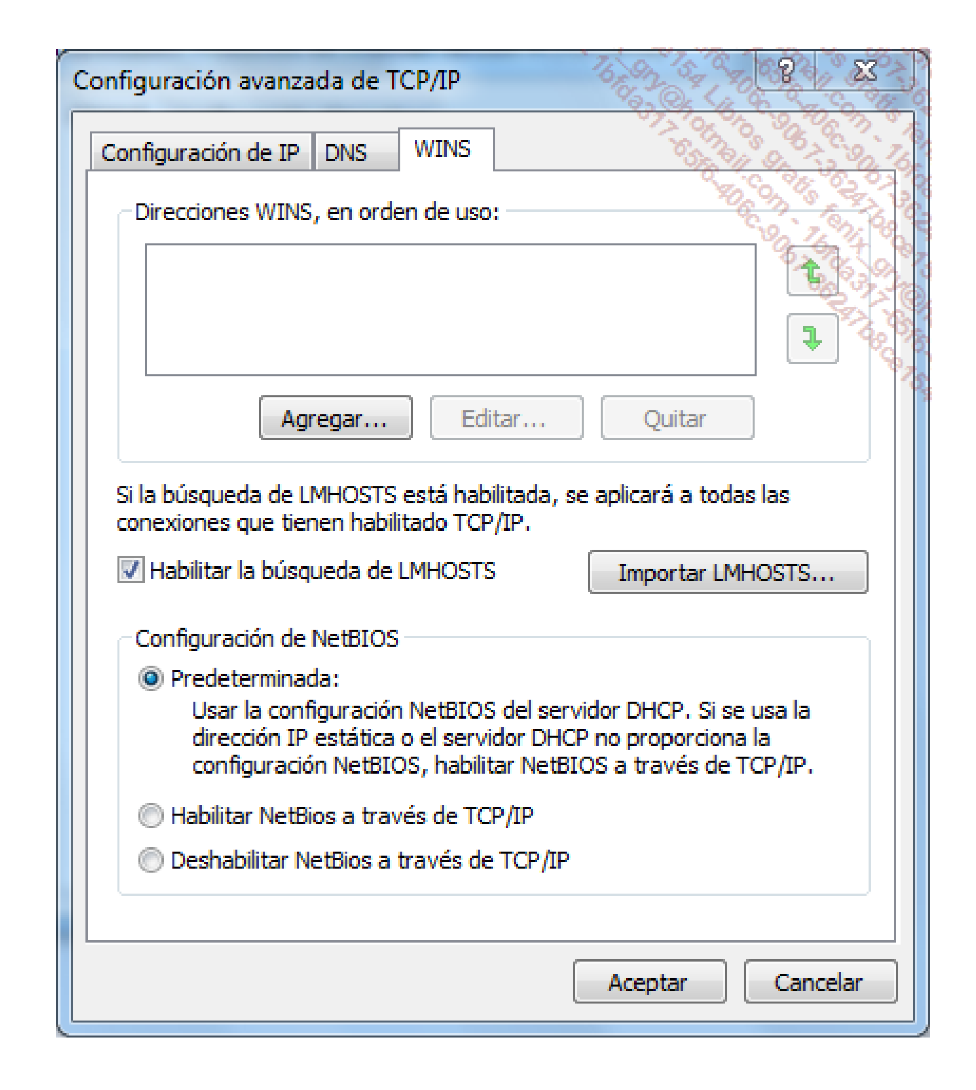
c. Los nombres NetBIOS

Utilización

Una estación de trabajo o un servidor Windows se pueden localizar por su nombre NetBIOS, de 15 caracteres, más un 16.º de identificación del servicio.

Los nombres NetBIOS se resuelven por medio de difusiones, utilizando un archivo local LMHosts o a través de un servidor *Windows Internet Name Service* (WINS).

Utilizar o no NetBIOS con TCP/IP se puede definir en la Configuración avanzada de TCP/IP:



Configuración de la resolución NetBIOS con TCP/IP

Observe que un ordenador UNIX/Linux no responde nunca a una petición de resolución de nombre NetBIOS por difusión, al contrario de lo que pasa con un ordenador que tiene un sistema operativo de Microsoft.

Constitución

En una red NetBIOS, cada ordenador debe disponer de un nombre único de 15 caracteres como máximo.

Los nombres NetBIOS puede contener todos los caracteres alfanuméricos, además de los siguientes: ! @ # $ % ˆ & ( ) - _ ’ { } . ~

No se pueden utilizar caracteres que se puedan asociar a caracteres genéricos, como el asterisco o la interrogación.

Se aconseja no utilizar espacios en los nombres NetBIOS, aunque algunas aplicaciones los pueden manejar. Así, se puede utilizar el siguiente comando, siempre que se envíen los parámetros entre dobles comillas:

```
Net view "\\EL SERVIDOR"
```

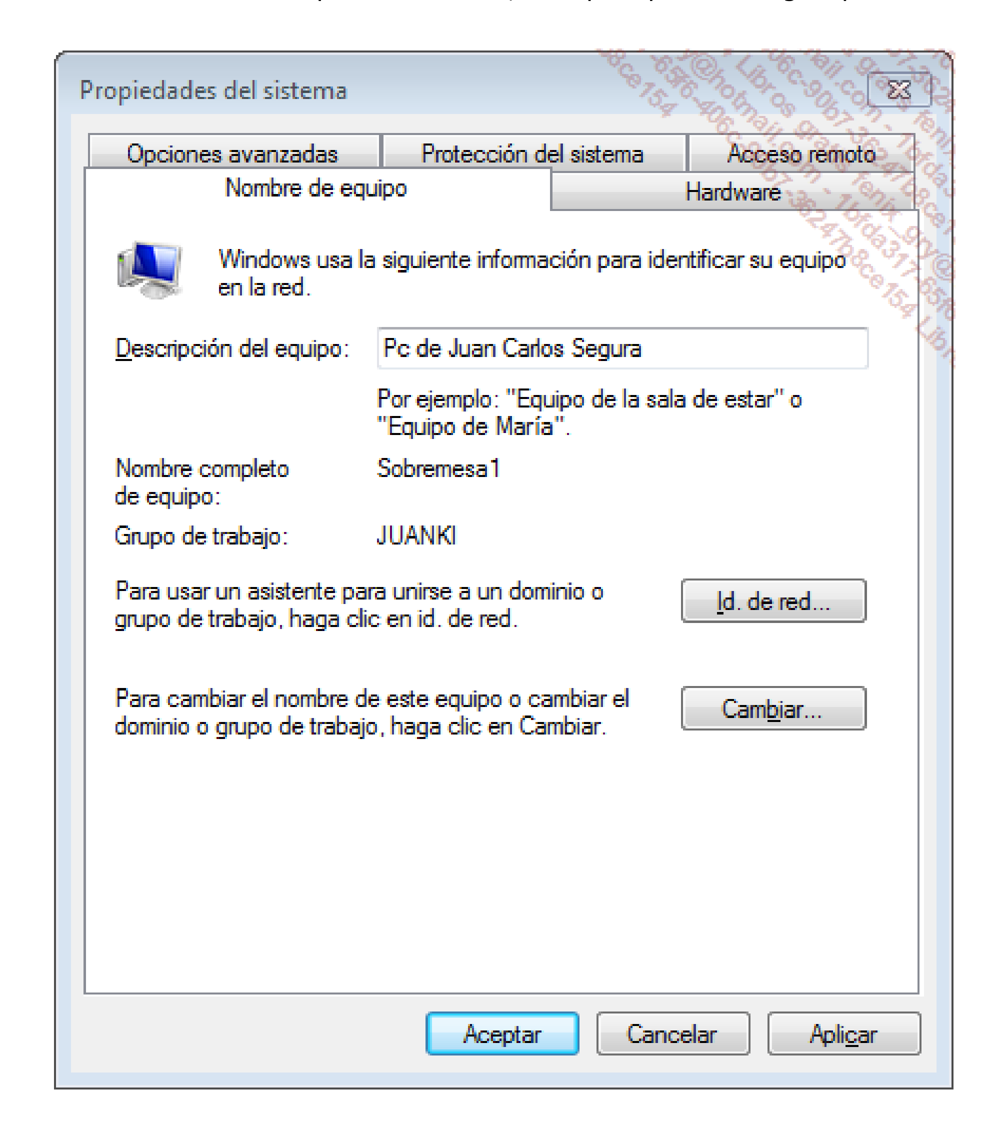
Implementación de una nomenclatura NetBIOS

Es necesario establecer una denominación para cada equipo, del tal modo que facilite su

identificación. Por ejemplo, se puede considerar una denominación en función de su ubicación física, de su sistema operativo o del usuario que trabaja con el equipo.

Configuración de un nombre NetBIOS de ordenador

Es necesario introducir un nombre para el ordenador durante la instalación del sistema operativo. El nombre se puede modificar en cualquier momento, siempre que se tengan permisos.



Nombre completo del ordenador Windows

Este nombre NetBIOS sirve para construir identificadores para las aplicaciones NetBIOS que se ejecutan localmente en el ordenador. Esto nombres son accesibles en un ordenador que disponga de un sistema operativo Windows que ejecute NBT (*NetBIOS over TCP/IP*).

Por ejemplo, a partir de la línea de comando en un ordenador con Windows, obtenemos la siguiente lista de nombre registrados localmente y en remoto en un servidor Windows de red.

```
C:\>nbtstat -n
Conexión de área local:
Dirección IP: [172.17.207.89] ID de ámbito : []
                Tabla de nombres locales NetBIOS
       Nombre                Tipo          Estado
    ---------------------------------------------
    DYONISOS              Único        Registrado
    DYONISOS        <20>  Único        Registrado
    ESCUELA         <00>  Grupo        Registrado
    ESCUELA         <1E>  Grupo        Registrado
C:\>nbtstat -a 172.17.0.100
Conexión de área local:
```

```
Dirección IP: [172.17.0.100] ID de ámbito: []
    Tabla de nombres NetBIOS de ordenadores remotos
       Nombre            Tipo         Estado
    ---------------------------------------------
    ULYSSE                Único        Registrado
    ENI-ESCUELA     <00>  Grupo        Registrado
    ULYSSE                Único        Registrado
    ULYSSE                Único        Registrado
    ENI-ESCUELA     <1E>  Grupo        Registrado
    INet~Services   <1C>  Grupo        Registrado
    IS~ULYSSE       <00>  Único        Registrado
    Dirección MAC = 00-50-FC-1F-3C-6F
C:\>
```

He aquí algunos identificadores NetBIOS habituales: NombreOrdenador <03> Servicio mensajería (instantánea), NombreOrdenador <00> Cliente para redes Microsoft y NombreOrdenador <20> Compartir archivos, impresión Microsoft.

3. TCP/IP

a. Antecedentes

La red ARPANET, nombre de la organización militar *Advanced Research Projects Agency* (ARPA) nació en 1969. La creó el *Department of Defense* (DoD), de EE. UU., para conectar diferentes sitios informatizados y en un primer momento conectó cuatro institutos universitarios. Se conectaron progresivamente una serie de centros militares y de investigación, públicos y privados, que participaron activamente en esta implementación.

A principios de los años setenta, Bob Kahn, del *Defense ARPA* (DARPA), ex-ARPA, trabajó con Vinton Cerf, investigador del Stanford Institute, en nuevos protocolos que permitieran conectar redes. Así nació TCP/IP. En 1976, ARPANET migra a TCP/IP. En 1978, una segunda red se conecta a ARPANET; utiliza las líneas telefónicas y toma el nombre de Internet.

Hoy en día, ARPANET es una parte de Internet que el DoD utiliza para Investigación y desarrollo.

La integración de los protocolos de Internet en el Unix *Berkeley Software Distribution* (BSD) y la difusión casi gratuita en las universidades contribuyó a mejorar el éxito de esta suite.

b. La suite de protocolos

La familia TCP/IP, de la que participan decenas de protocolos, define un modelo en cuatro capas de red.

Se trata los de protocolos de comunicación y de aplicación más conocidos para conectar sistemas heterogéneos, independientemente de la capa física.

Transmission Control Protocol (TCP) es un protocolo de transporte que asegura un servicio fiable, orientado a la conexión para un flujo importante de bytes.

Al contrario que TCP, *User Datagram Protocol* (UDP) es el protocolo de transporte no orientado a la conexión. Es más rápido pero menos fiable.

Internet Protocol (IP) proporciona un sistema de entrega de paquetes, sin conexión y no fiable. Administra las direcciones lógicas, que dividen el identificador del nodo en un número de red lógico y un número de dispositivo de 4 bytes (en IP versión 4).

El protocolo IPv6, o IP *Next Generation* (NG), está disponible en los sistemas operativos más recientes.

Una de las claves del éxito de los protocolos de Internet reside en el hecho de que el modelo propuesto es independiente de las capas Física y de Conexión de datos (capas 1 y 2 del modelo OSI).

c. Correspondencia con el modelo OSI

Es importante recordar que el modelo TCP/IP se propuso diez años antes que el modelo OSI, y que este se inspiró mucho en algunos protocolos de TCP/IP; sin embargo, cabe remarcar que el modelo OSI define un modelo de 7 capas y que los protocolos de Internet funcionan sobre cuatro.

Modelo OSI	Modelo TCP/IP				
5-6-7	Aplicación	Telnet	ftp	dns	snmp
		Windows Sockets			
4	Transporte	TCP		UDP	
3	Internet	IP	ICMP		
		ARP			
1-2	Interfaz de red	Ethernet	Token Ring	Otros	

d. La implementación en las empresas

Las cualidades de la suite de protocolos TCP/IP, como su capacidad de funcionamiento en cualquier tamaño de red, su eficacia y su carácter evolutivo, hacen que las empresas muestren gran interés por estos protocolos. Inicialmente, interconectaban las redes a través de Internet, sobre todo para aplicaciones de servicio de mensajería y Web.

Poco a poco, se han ido adoptando estos protocolos, estandarizados y no vinculados a ningún fabricante o editor específicos, dentro de las redes locales. Las intranet han comenzado a expandirse, utilizando los mismos protocolos y principios que Internet y, como el anonimato es una de sus características, se ha hecho necesario implementar la autentificación del empleado para que pueda acceder a su empresa.

El nombre extranet designa la capacidad que tiene el usuario de acceder a la red local de tipo intranet desde fuera. Aplicando siempre las mismas normas a nivel de red, la autentificación permite reconocer a los usuarios externos de la empresa, que tendrán menos privilegios.

Protocolo IP versión 4

1. Principios

IP genera una entrega de paquetes sin conexión y sin garantía. Uno de sus principales inconvenientes es que necesita la implementación de un plan de direccionamiento explícito. Cada nodo de red se tiene que identificar con una dirección IP. Esta se divide en dos partes: un número de red lógico y una dirección de equipo en la red lógica.

Se podría representar el número de red IP como el nombre de una calle y el número de servidor como una dirección de esa calle.

Uno de los aspectos interesantes de IP es que se puede configurar para que se garantice un tipo de servicio específico. Entre estos, se puede citar la implementación de un envío urgente de un paquete que se debe transmitir rápidamente, o de políticas para incrementar la velocidad cuando se debe transferir una gran cantidad de información, o bien optimizar la fiabilidad en la transmisión para un flujo en el que no se puede permitir que haya ningún error.

2. Direccionamiento

a. La dirección IPv4

La utilización de TCP/IP requiere que el administrador defina un plan de direccionamiento, asignando una dirección IP para cada nodo activo de red.

Una dirección IP versión 4 se representa con 4 bytes. Se utiliza la notación decimal punteada, es decir, cada byte se separa con un punto: 132.148.67.2

Según el valor del primer byte, es posible conocer la clase de dirección IP, es decir, el número de bytes utilizados para el número de red y los que quedan para el equipo.

Esto no siempre es cierto. De hecho, es posible, en algunos casos, recurrir al *subnetting*,es decir, se utiliza una parte de los bits del servidor pertenecientes a cierta clase para cifrar un número de subred. Se habla de *supernetting* cuando es una parte del número de red de la clase predeterminada la que se utiliza para cifrar equipos suplementarios.

b. La máscara

Enfoque directo

Se utiliza una máscara de red secundaria para identificar la parte de la dirección IP que corresponde a la red, de la parte que identifica al nodo. Si se escribe la dirección IP en forma binaria, cualquier bit asociado al número de red se representará como '1' en la máscara y como '0' si no está asociado.

Un byte cuyo valor binario es 1111 1111 equivale a 255 en decimal. Como la dirección IP se representa con 4 bytes (32 bits), las máscaras pueden ser:

- 255.0.0.0
- 255.255.0.0
- 255.255.255.0

Más adelante veremos que una máscara no puede tomar como valor 255.255.255.255.



Enfoque computacional

La tarjeta de red o el router que ejecuten IP efectuarán un cálculo simple para encontrar el número lógico de red:

RL = IP Y máscara binaria

En la calculadora de Windows en modo «Programador», el Y binario se representa con el operador «And».

Así, si A dispone de la siguiente información:

IPA = 131.107.8.1

mA = 255.255.0.0

RLA = IPA Y mA

RLA = 131 Y 255 . 107 Y 255. 8 Y 0. 1 Y 0

Luego RLA = 131.107.0.0

La descomposición opera como en la clase B, en dos bytes para el número de red y dos bytes para el número de equipo.

Si ahora la máscara utilizada es 255.255.255.0, el número de red lógico es el siguiente:

RLA = 131 Y 255. 107 Y 255. 8 Y 255. 1 Y 0

O sea:

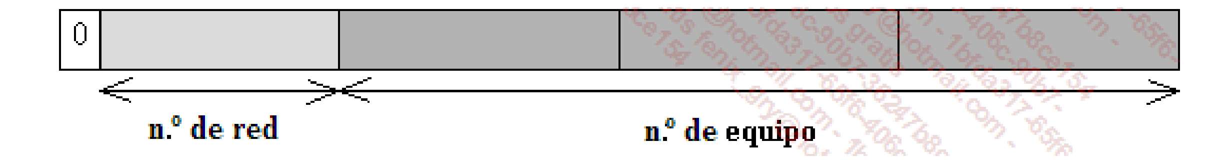
RLA = 131.107.8.0 y la descomposición opera en 3 + 1.

c. Clases de direcciones

Clases

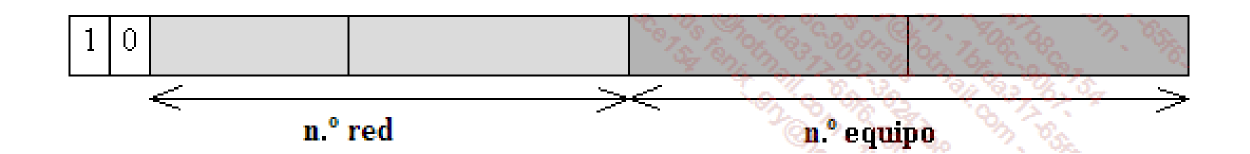
Para identificar un equipo de manera única, se definen tres clases de direcciones.

Clase A, el primer byte se ubica entre 1 y 126. Se utilizan 7 bits para el número de red y 24 bits para identificar el equipo. Una red de clase A puede soportar hasta 16 millones de equipos (2^{24}-2 posibilidades).



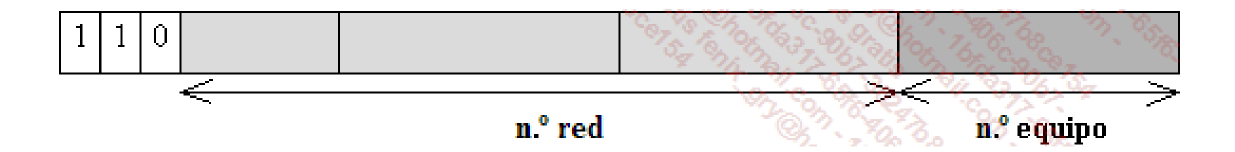
Por ejemplo, 112.2.1.4 es una dirección de clase A. '112' define el número de red y '2.1.4' el número de equipo.

En una clase B, el primer byte varia entre 128 y 191. Con 14 bits se hace el cifrado del número de red y con 16 bits el número de equipo. Se puede definir hasta 65.534 equipos en una misma red (2^{16}-2). La máscara por defecto es 255.255.0.0.



132.148.67.2 es de clase B. '132.148' es el número de red y '67.2' el número de equipo.

La clase C está definida por un primer byte variable de 192 a 223. Se utilizan 21 bits para la red y 8 para el equipo. Podemos tener hasta 254 equipos por red en clase C.



193.10.2.117 es de clase C. '192.10.2' es la parte que identifica la red y '117' el equipo.

Direcciones particulares

Un número de red o un número de equipo no pueden tener todos sus bits en 0 o en 1. Estos casos particulares se reservan para situaciones concretas.

Por ejemplo, para una difusión, todos los bits del «equipo» de la dirección IP se ponen a '1'.

Por ejemplo, la dirección 132.148.255.255 identifica a todos los equipos de la red 132.148.

Hay que tener en cuenta que en algunos sistemas Unix es posible configurar una difusión con todos los bits en '0', para mantener la compatibilidad con otros sistemas.

El número de red actual se anota poniendo todos los bits del equipo en '0'.

Por ejemplo, 132.148.0.0 se asocia con el número de red lógico 132.148.

A veces se puede identificar una estación de la red sustituyendo el número de red por '0'.

Por ejemplo, 0.0.67.2 corresponde al equipo 132.148.67.2 de la red 132.148.0.0.

En cuanto a la dirección de bucle local 127.0.0.1, pertenece a la propia tarjeta de red, sin salir a la red.

d. Direcciones privadas

Hay un cierto número de direcciones IP que se reservan para utilizarlas en la red interna. Estas direcciones definidas en RFC 1918 permiten asegurar a un servidor Proxy (que administra la conexión a Internet de una empresa) una diferenciación satisfactoria entre la red pública (Internet) y la red privada (intranet). Así, cada empresa conectada a Internet puede utilizar las mismas direcciones IP privadas internamente y diferenciar los accesos a Internet por medio de una única dirección IP pública externa.

Estas direcciones IP privadas son:

- 10.0.0.0 en 10.255.255.255.
- 172.16.0.0 en 172.31.255.255.
- 192.168.0.0 en 192.168.255.255.

e. Las direcciones APIPA

Microsoft utiliza la Asignación Automática de IP Privadas o *Automatic Private IP Addressing*(APIPA) para proporcionar una dirección IP a un ordenador que no encuentra un servidor DHCP. De este modo, todos los ordenadores que están en la misma situación, a pesar de todo, podrán comunicarse entre ellos.

Este rango de direcciones va de 169.254.0.0 a 169.254.255.255.

Los dos últimos bytes de la dirección se generan utilizando como entrada la dirección MAC, que inicializa el algoritmo de generación aleatoria. La RFC 3927 describe las características de APIPA: http://tools.ietf.org/html/rfc3927

3. El direccionamiento sin clase

a. Principios

Con el creciente aumento del número de ordenadores conectados a Internet, las direcciones IP versión 4 aún disponibles se hacen cada vez más escasas. Gracias a la generalización de la utilización de servidores Proxy y rangos de direcciones IP privadas (RFC 1918), ha sido posible añadir grupos de miles de ordenadores, simplemente asignando una dirección IP pública al Proxy. Así, la escasez de IP se hace menos problemática de lo que se había previsto.

Sin embargo, la descomposición en clases generó un derroche colosal de direcciones, que se ha evitado reasignando algunos rangos.

Por ejemplo, imaginemos que a una empresa se le ha asignado un rango de direcciones de 60.0.0.0 a 60.255.255.255 y que, en realidad, solo utiliza desde la subclase 60.1 a 60.10. ¿Cómo hacer para recuperar las direcciones 60.11 a 60.255?

Basta con considerar las direcciones IP no como de clase A, sino más bien de clase B. Así, un router sabrá diferenciar entre las direcciones del primer tramo y las del segundo tramo.

Consideremos ahora que las clases de direcciones ya no existen y que, por lo tanto, la máscara utilizada no es necesariamente la de la clase predeterminada.

Por ejemplo, una empresa que quiere poner en línea algunos servidores puede pedir que se le asigne el siguiente rango de 8 direcciones: 61.178.203.56 a 61.178.203.63. Se le proporcionará con una máscara 255.255.255.248 (es decir, que 5 bits del 4.° byte se utilizarán para las redes y 3 bits para los huéspedes). El prefijo correspondiente es 61.178.203.56. El último byte, escrito en binario, proporciona los siguientes valores:

56 = 0011 1000

57 = 0011 1001

58 = 0011 1010

59 = 0011 1011

60 = 0011 1100

61 = 0011 1101

62 = 0011 1110

63 = 0011 1111

Los 5 bits de peso del último byte se asocian a una parte que define el número lógico de red.

Una máscara 255.255.255.248 en binario corresponde a 1111 1111.1111 1111.1111 1111.11111000.

11111000 representa la escritura binaria del último byte de la máscara y equivale a 248 (128 + 64 + 32 + 16 + 8).

b. La notación CIDR

La notación *Classless InterDomain Routing* (CIDR) ofrece una escritura sintética de la máscara de red secundaria.

Así, si la máscara es 255.0.0.0, significa que habrá 8 bits en 1 para la escritura binaria de la máscara, lo que se escribirá como /8.

Generalmente se anotará como **/n**, donde n representa el número de bits en 1 de la máscara, es decir, el número de bits de la dirección IP que servirán para cifrar una parte de la red lógica.

En la mayoría de los casos, los bits en 1 de la máscara serán los bits de peso (los del extremo izquierdo) y nunca se debe confundir el 1 con el 0 en la máscara.

Así, la máscara 255.255.0.0 se escribirá /16 en notación CIDR.

La máscara 255.255.255.0 se escribirá /24.

Según el ejemplo anterior, la máscara 255.255.255.248 se escribirá /29.

La utilización de una asignación de direcciones sin clase ofrece una descomposición de las direcciones IP por medio de máscaras /8 a /30.

Algún hardware implementa la introducción de la máscara en notación CIDR.

c. El papel de la máscara de red

Inicio de un paquete de datos

En el capítulo Estandarización de protocolos, hemos visto que una tarjeta de red comprueba si el destinatario se encuentra en la misma red lógica. Según sea el caso, esta tarjeta de red recurre a la puerta de enlace predeterminada o se dirige directamente a su destinatario.

Llamemos A al emisor. Conoce su dirección IP (IPA), su máscara (mA) y la dirección física de la tarjeta de red (PHYA).

Como emisora del paquete de datos, esta máquina A solo conoce del destino la dirección IP. En las explicaciones siguientes, denominaremos B al equipo de destino, y a su dirección IP, IPB.

Para poder enviar el paquete de datos, A tiene que saber, en primer lugar, si la red lógica de B (RLB) es la misma que la suya (RLA). Ahora bien, A solo conoce la dirección IPB, pero no la máscara correspondiente. Por lo tanto, le es imposible encontrar RLB directamente.

Por eso A tiene que encontrar un modo de encontrar RLB. Para ello, A utiliza su propia máscara mA, conjuntamente con la dirección IPB. Efectúa su propia interpretación de lo que podría ser RLB.

Tampoco podemos olvidar el tratamiento de nivel 2. En efecto, A y B pueden o no estar sobre la misma red.

Citaremos para los siguientes ejemplos el protocolo ARP, que se explicará más adelante. Por ahora, debemos saber que ARP permite interrogar a la red de difusión para encontrar la dirección de nivel 2 de una estación y establecer la relación con su dirección IP. Para no efectuar sistemáticamente esta consulta, se mantiene una caché que permite guardar una lista de direcciones MAC y sus direcciones IP correspondientes.

Teóricamente, se pueden identificar cuatro casos:

1) A interpreta RLB como equivalente a RLA y A y B están en la misma red de nivel 2.

2) A interpreta RLB como no equivalente a RLA y A y B están en la misma red de nivel 2.

3) A interpreta RLB como equivalente a RLA y A y B no están en la misma red de nivel 2.

4) A interpreta RLB como no equivalente a RLA, A y B no están en la misma red de nivel 2.

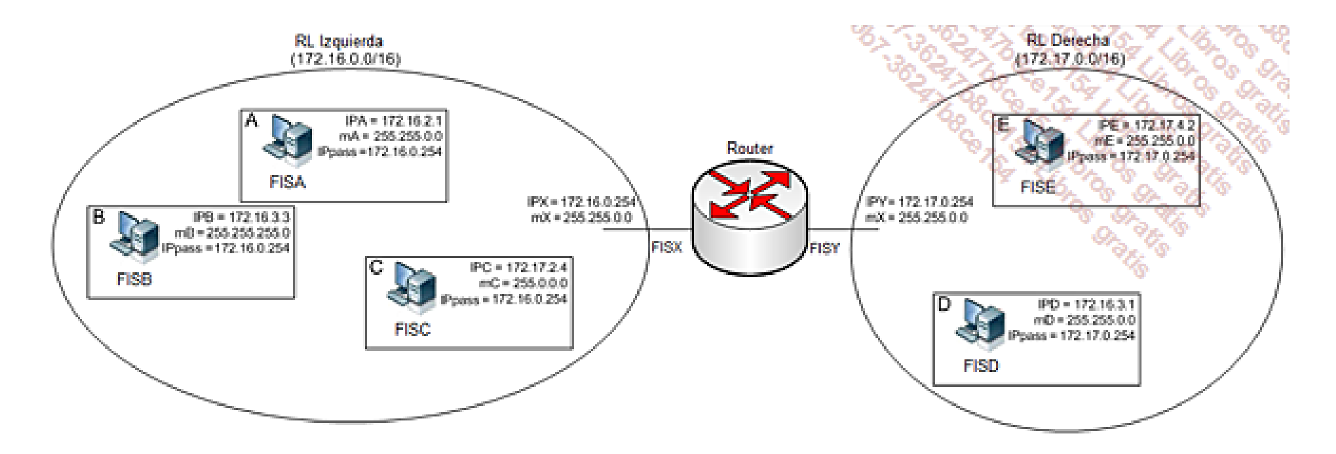
Podemos señalar que el tercer caso parece incoherente. De hecho, puede parecer ilógico prolongar una misma red IP más allá del espacio de difusión de nivel 2.

Vamos a estudiar las interpretaciones de direcciones con ejemplos sencillos: el funcionamiento de una consulta «ping». La comunicación es necesariamente doble, con el tratamiento de la ida (pregunta) y el de la vuelta (retorno) de los paquetes de datos.

Incidencias de máscaras erróneas sobre la distribución de los paquetes de datos IP

Aquí vamos a examinar una comunicación en una red que dispone de una asignación de direcciones incorrecta o de máscaras erróneas.

En la configuración que se presenta a continuación, podemos observar que mA, mB y mC son distintas entre sí. Además, mB y mC no corresponden a la máscara del router (puerta de enlace) mX. La red lógica que puede ser determinada al nivel de la puerta de enlace es 172.16.0.0. Observemos que la IPC no puede corresponder a una dirección en esta red lógica. Por el otro lado de nuestro router, RLD es diferente a RLE y RLY.



Vamos a explicar esta arquitectura para estudiar la incidencia de una máscara errónea en la distribución de los paquetes de datos. Para ello vamos a desglosar los mecanismos subyacentes relacionados con la instalación de la comunicación.

Envío de A hacia B

Como hemos visto anteriormente, el emisor A trata de comparar su red lógica con la del destinatario B. Los datos de cada uno son los siguientes:

IPA = 172.16.2.1 y mA = 255.255.0.0, por lo que RLA es igual a 172.16.0.0.

IPB = 172.16.3.3 y mA = 255.255.0.0, por lo que RLB visto por A es igual a 172.16.0.0.

Observamos que hay igualdad entre RLA y RLB supuesta por A. Por otra parte, A y B están en la misma red de nivel 2. Por este motivo es normal considerar que A y B estén en la misma red lógica.

Para crear su paquete de datos, A busca en primer lugar la dirección de nivel 2 (MAC) de B. Si no dispone de esta información en memoria, difunde una consulta de nivel 2, ARP. Esta consulta llegará al conjunto de equipos de la parte izquierda del diagrama. El router bloquea esta difusión.

Cuando dispone de su propia dirección física y de la de B, A emite una trama de FISA hacia FISB

(nivel 2) y un paquete de datos de IPA hacia IPB (nivel 3).

El destinatario B recibe los datos.

Envío de B hacia A

El proceso es igual que en el caso anterior: B intenta encontrar la red lógica de A para compararla con la suya.

IPB = 172.16.3.3 y mB = 255.255.255.0, por lo que RLB es igual a 172.16.3.0.

IPA = 172.16.2.1 y mB = 255.255.255.0, por lo que RLA visto por B es igual a 172.16.2.0.

Observamos que la asignación de direcciones de nivel 3 es diferente entre los dos equipos, aunque pertenecen a la misma red de difusión y parecen pertenecer a la misma subred IP. Esto parece poco lógico.

Tanto es así que B, al constatar que debe cambiar de red lógica para llegar a A, se dirige a la IP de enlace, el router de la red lógica.

En primer lugar, se debe conocer a través de una consulta ARP de la caché correspondiente de B la dirección física FISX correspondiente a IPX. La trama está construida de FISB hacia FISX, para dirigir la información hacia el router. El paquete de datos, por su parte, informa que IPB es el emisor e IPA el destinatario.

Una vez que ha llegado al router, este debe tratar la información.

Distribución de un paquete de datos a través del router

Cuando recibe el paquete de datos, el router consulta su tabla de transporte para encontrar una ruta que corresponda a la red supuesta de A, aplicando la máscara especificada.

La siguiente tabla de transporte es la de un ordenador Linux equipado con dos tarjetas de red que simula nuestro router.

```
[root@linus /root]# netstat -rn
Kernel IP routing table
Destination    Gateway       Genmask          Flags MSS Window  irtt Iface
172.17.0.2     0.0.0.0         255.255.255.255 UH        0 0       0 eth0
192.168.6.0    172.16.206.1    255.255.255.0   UG        0 0       0 eth1
192.168.5.0    172.16.205.1    255.255.255.0   UG        0 0       0 eth1
192.168.4.0    172.16.104.1    255.255.255.0   UG        0 0       0 eth1
192.168.3.0    172.16.103.1    255.255.255.0   UG        0 0       0 eth1
192.168.2.0    172.16.102.1    255.255.255.0   UG        0 0       0 eth1
192.168.1.0    172.16.101.1    255.255.255.0   UG        0 0       0 eth1
192.168.16.0   172.16.206.1    255.255.255.0   UG        0 0       0 eth1
192.168.15.0   172.16.205.1    255.255.255.0   UG        0 0       0 eth1
192.168.14.0   172.16.104.1    255.255.255.0   UG        0 0       0 eth1
192.168.13.0   172.16.103.1    255.255.255.0   UG        0 0       0 eth1
192.168.12.0   172.16.102.1    255.255.255.0   UG        0 0       0 eth1
192.168.11.0   172.16.101.1    255.255.255.0   UG        0 0       0 eth1
10.108.2.0     172.17.208.208  255.255.255.0   UG        0 0       0 eth0
192.168.8.0    172.16.208.1    255.255.255.0   UG        0 0       0 eth1
172.16.0.0     0.0.0.0         255.255.0.0     U         0 0       0 eth1
172.17.0.0     0.0.0.0         255.255.0.0     U         0 0       0 eth0
127.0.0.0      0.0.0.0         255.0.0.0       U         0 0       0 lo
[root@linus /root]#
```

En la red 172.16, se declaran varias rutas que permiten el acceso a otras redes lógicas.

Por ejemplo, se puede acceder a las redes 192.168.5.0/24 y 192.168.15.0/24 a partir del router que tiene la dirección IP 172.16.205.1, en la red 172.16.0.0/16.

 Para identificar una dirección de destino exacta con relación a una entrada de la tabla de

enrutamiento, se utiliza una máscara 255.255.255.255, es decir, que la dirección IP comparada deberá volver a dar exactamente la dirección IP examinada.

Por el contrario, se definirá una ruta predeterminada con 0.0.0.0 con una máscara 0.0.0.0. Cualquiera que sea la dirección de destino examinada, encontrará inevitablemente el resultado 0.0.0.0. Esta ruta ineludiblemente se examina en último lugar en un tabla y corresponde a una clase de itinerario BIS o de «Otras direcciones» en un router.

De esta manera, el router conoce la existencia de las redes lógicas 172.16.0.0/16 (izquierda) y 172.17.0.0/16 (derecha). Dispone de sus propias máscaras para las redes lógicas que conoce.

Cuando recibe el paquete de datos, el router compara las rutas y se da cuenta de que la red lógica de A está a la izquierda. Entonces, reconstruye un paquete de datos utilizando IPA y PHYA.

La información llegará a su destino, incluso aunque la dirección lógica parezca errónea. Por el contrario, aunque A y B estén en la misma red de nivel 2, no pueden comunicarse directamente y la información tiene que circular por el router.

Envío de A hacia C

Después de superponer su máscara en IPC, A ve a C en una red lógica distinta de la suya y por tanto se dirige al router. Sin embargo, al contrario que en el caso anterior, el router envía el paquete de datos por el lado derecho a la red lógica 172.17.0.0. El equipo C no puede responder a la consulta ARP porque no está en esa red lógica. Por lo tanto, la información no se puede transmitir al destinatario final.

Envío de A hacia D

A interpreta la dirección IPD como si estuviera en la misma red lógica que la suya, IPA. Por lo tanto, intenta dirigir directamente la información mediante una difusión ARP. Esta no puede pasar el router y no llega a destino. La comunicación se detiene.

Envío de A hacia E

Este caso presenta una coherencia completa en cuanto a asignación de direcciones lógica respecto al espacio de difusión. El paquete de datos se envía al router y llega a su destino.

d. La descomposición en subredes

Contexto

Primera hipótesis

Imaginemos que trabajamos en una gran empresa que dispone de varios emplazamientos, una sede y cinco sucursales. Cada sucursal se conecta a Internet pasando por la sede por medio de una conexión dedicada. Solo la sede dispone de conexión directa a Internet.

Somos los responsables de la implementación del plan de asignación de direcciones a nivel local. Por ejemplo, el arquitecto que definió el plan de asignación de direcciones nacional nos impone utilizar un único rango de direcciones privadas (según la RFC 1918), que es 172.16.0.0 - 172.16.255.255.

Ahora bien, *in situ* tenemos un gran número de puestos de red y varios routers.

Necesariamente debemos utilizar este prefijo impuesto para efectuar una descomposición de este rango en varios rangos distintos para cada una de las redes lógicas.

Segunda hipótesis

Nos asignan un pequeño rango de direcciones IP públicas para publicar servidores en Internet. Sin embargo, a causa de la infraestructura de red existente, debemos utilizar este único rango de direcciones para desplegar dos rangos en vez de uno.

Primera solución (enfoque intuitivo)

Imaginemos que en la sucursal deben disponer de 5 redes lógicas. Por tanto, debemos dividir el rango que tenemos en 5 rangos de direcciones.

Una primera solución sencilla y evidente consiste en pasar de un identificador de red lógico cifrado de 2 bytes a un identificador cifrado de 3 bytes.

Así, podríamos tener:

- RL1 = 172.16.1.0/24, como rango de direcciones 172.16.1.0 a 172.16.1.255.
- RL2 = 172.16.2.0/24, como rango de direcciones 172.16.2.0 a 172.16.2.255.
- RL3 = 172.16.3.0/24, como rango de direcciones 172.16.3.0 a 172.16.3.255.
- RL4 = 172.16.4.0/24, como rango de direcciones 172.16.4.0 a 172.16.4.255.
- RL5 = 172.16.5.0/24, como rango de direcciones 172.16.5.0 a 172.16.5.255.

Estos rangos son teóricos. Hay que reservar las direcciones utilizables: aquellas en las que todos los bits del equipo son 0 o 1. Los rangos irán realmente de 172.16.x.1 a 172.16.x.254.

Una red lógica 172.16.0.0/16 tiene 65.534 (216 - 2) direcciones IP utilizables.

Estas redes lógicas con una máscara de 24 bits solo pueden direccionar 254 direcciones IP cada una, es decir, 5 x 254 = 1270 direcciones.

La diferencia con las direcciones utilizables es notable. Como contrapartida, la máscara de clase C simplifica este planteamiento.

Por el contrario, a menos que necesitemos 254 redes lógicas, la pérdida de direcciones IP es muy elevada.

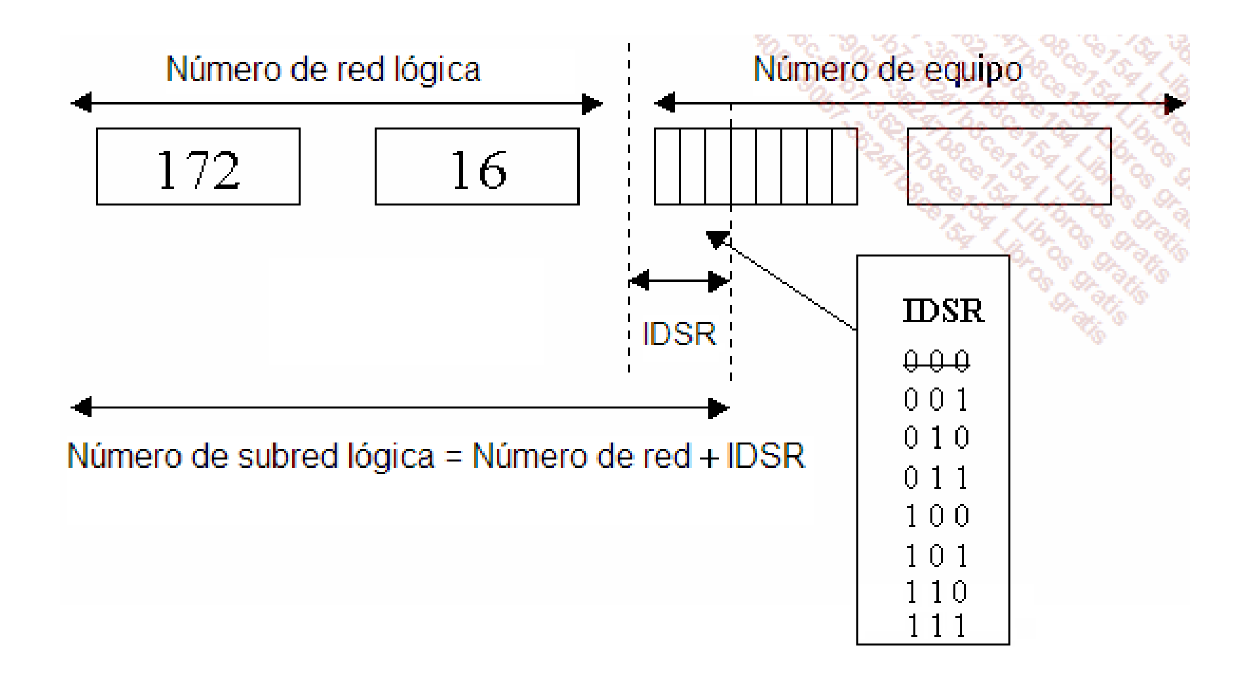
Segunda solución (la buena)

Hipótesis básica

Ahora, el objetivo consiste en encontrar una descomposición que optimice el número de redes secundarias requeridas. Si retomamos el ejemplo anterior, se busca una codificación que permita conservar un máximo de equipos en función del número de redes lógicas.

Por ejemplo, dada una subred 172.16.0.0 y un número de redes lógicas NmRL = 5, y considerando que el número máximo de equipos por red lógica es NmH = 200, ¿cuántos bits de la parte equipo inicialmente disponible son necesarios para cifrar NmRL redes lógicas?

Cada una de estas RL será de hecho una subred, cuyo número está compuesto por el de la red lógica y el identificador de subred (IDSR).



Etapa 1: cálculo del número de bits para cifrar el número de redes lógicas

Es necesario encontrar el número de bits (NmBITS) necesario para cifrar el número de redes lógicas (NmRL).

NmRL tiene que ser inferior o igual a 2^{NmBITS}.

Para simplificarlo, a continuación se puede ver un cuadro para realizar los cálculos.

La primera columna indica el número de bits utilizados (NmUtil).

La segunda expresa el número de posibilidades de cifrado para NmUtil (NmPos). La primera línea muestra dos posibilidades, 0 o 1. La siguiente línea se multiplica por 2.

La tercera columna, NmRetenidos, contiene el número de direcciones realmente utilizadas una vez hemos eliminado todas aquellas en que todos los bits son 0 o 1. Para esto, siempre se resta 2 de la anterior.

Tenga en cuenta que, desde la RFC 1878, un identificador de subred (IDSR) puede tener todos sus bits a 0 o todos sus bits a 1. Sin embargo, determinado hardware no actualizado puede ser un problema en este caso. No lo tendremos en cuenta para nuestros cálculos.

mSRbin representa en binario la máscara de subred lógica, a partir del tercer byte. mSRdec da la misma información en formato decimal.

Lo que nos da el siguiente cuadro:

NmUtil	NmPos	NmRetenidos	mSRbin	mSRdec
1	2	0	1000 0000	128
2	4	2	1100 0000	192
3	**8**	**6**	**1110 0000**	**224**
4	16	14	1111 0000	240
5	32	30	1111 1000	248
6	64	62	1111 1100	252
7	128	126	1111 1110	254
8	256	254	1111 1111	255
9	512	510	11111 1111. 1000 0000	255.128

10	1024	1022	11111 1111. 1100 0000	255.192
11	2048	2046	11111 1111. 1110 0000	255.224
12	4096	4094	11111 1111. 1111 0000	255.240
13	8192	8190	11111 1111. 1111 1000	255.248

El valor que debemos encontrar para NmBits lo encontramos en el cuadro buscando en la columna NmRetenidos el valor inmediatamente superior o igual.

En el ejemplo, para NmRL = 5, el valor correspondiente es NmRetenido = 6, y por tanto NmUtil = NmBITS = 3, que es el valor que leemos en la misma línea.

El cuadro nos indica que son necesarios 3 bits para cifrar 5 subredes lógicas.

Etapa 2: obtención de la máscara CIDR

La máscara en notación CIDR se obtiene sumando al valor inicial el número de bits encontrados.

Así, /16 + 3 pasa a ser /19.

Etapa 3: obtención de la máscara decimal

Al leer el cuadro, en la columna mSRbin y mSRdec, es fácil leer el byte en binario o en decimal que corresponde a la máscara.

En este ejemplo, la máscara retomará los 16 primeros bits del prefijo inicial, al cual se añadirá el byte mSRbin, y luego un byte a 0.

La máscara que se obtiene es 255.255.224.0.

Etapa 4: cálculo de los IDSR

Para enumerar los identificadores de subred (IDSR), basta con contar en binario de 0 a NmPos - 1.

Así, en el caso que nos ocupa, vamos a trabajar con 3 bits (NmBITS).

La enumeración nos lleva a:

Decimal	Binario en NmBITS
0	*000*
1	001
2	010
3	011
4	100
5	101
6	110
7	*111*

Etapa 5: obtención de los números de subred

El prefijo de los dos primeros bytes sigue siendo: 172.16.

El tercer byte comienza en binario por 001. Los dos últimos bytes variables en binario son: 001x xxxx.xxxx xxxx.

x representa un valor 0 o 1 asignado.

El identificador de subred lógica escrito en binario en realidad será un prefijo cifrado de 19 bits:

172	.16	.?	.0

10101100	.0001 0000	.001 x xxxx	.xxxx xxxx

Así, este tercer byte, al considerar el identificador de red secundaria lógico (todos los bits del equipo a 0), tendrá como valor:

0010 0000, o sea, 32 en decimal, y por tanto el valor 172.16.32 /19 para RL1.

Lo mismo sucede para el resto de las redes lógicas.

Para RL2:

172	.16	.?	.0
10101100	.0001 0000	.010 x xxxx	.xxxx xxx

Así obtenemos como tercer byte 0100 0000, o sea 64 en decimal y por tanto 172.16.64 /19 para RL2.

Del mismo modo:

- RL3 = 172.16.96.0/19
- RL4 = 172.16.128.0/19
- RL5 = 172.16.160.0/19
- RL6 = 172.16.192.0/19 (no solicitado en este caso)

Podemos observar que el identificador de subred lógica aumenta en 32 cada vez. Este valor se denomina **incremento**.

De hecho, esto ocurre porque, en binario, cuando se añade 0 a la derecha se multiplica por 2. Aquí añadimos 5 ceros, por lo tanto multiplicamos los valores numéricos decimales de 1 a 6 por 32 (=2^5= 2 x 2 x 2 x 2 x 2).

Etapa 6: expresión de los rangos de direcciones de redes secundarias

En esta última etapa, solo nos queda expresar todas las posibilidades, es decir, la lista de las direcciones IP que se asignarán a los equipos en el entorno de red.

A cada equipo se le asignará la misma máscara, cualquiera que sea la subred en cuestión, es decir /19 o 255.255.224.0 en decimal.

Finalmente, retomamos los números de red secundaria encontrados y exponemos todas las posibilidades:

- RL1 = 172.16.32.0/19
- RL2 = 172.16.64.0/19
- RL3 = 172.16.96.0/19
- RL4 = 172.16.128.0/19
- RL5 = 172.16.160.0/19

Para cada red lógica, expresaremos en binario la escritura de las direcciones del equipo. Para encontrar el valor más pequeño, todos los bits de la parte del equipo se ponen a 0. Para encontrar el valor más alto, pondremos todos los bits del equipo a 1.

Así, para RL1, tendremos:

172	.16	.32	.0
10101100	.0001 0000	.001 x xxxx	.xxxx xxxx

La dirección en que todos los bits del equipo están a 0 nos da:

Protocolo IP versión 6

1. Introducción

En 1992 el hecho de constatar la escasez de direcciones y el aumento de las tablas de enrutamiento dio lugar al inicio del proyecto IP Siguiente Generación (IP NG).

Se trataba igualmente de implementar de manera nativa las numerosas opciones disponibles con IPv4, trabajando en cuatro temas principales: la autoconfiguración, la movilidad, la implementación de multicast y sobre todo la seguridad (autentificación y confidencialidad).

En diciembre de 1995, se publicó la RFC 1883 «Internet Protocol Version 6».

Esta RFC tardó poco en considerarse obsoleta y se reemplazó por la RFC 2460 en diciembre de 1998 (http://tools.ietf.org/html/rfc2460).

En junio de 1998, nació una red experimental: la **6Bone** (troncal IPv6), para permitir probar IPv6 en condiciones reales. Esta red utilizaba los prefijos 3FFE::/16 (RFC 2471). Esta red se cerró el 6 de junio de 2006 (¡06/06/06!) una vez concluyó el experimento.

2. Principios

IPv6, o IP *Next Generation* (NG), es la nueva versión de IP (*Internet Protocol*), que debe sustituir al protocolo IPv4. Esta migración es progresiva pero se debe realizar rápidamente.

IPv6 mantiene las principales funcionalidades de su predecesor y además cubre sus carencias con la incorporación de nuevas funciones.

En primer lugar, se ha ampliado el espacio de asignación de direcciones de 4 bytes (32 bits) a 16 bytes (128 bits). Desde el principio, este era uno de los objetivos principales de esta nueva versión. De hecho, no se esperaba que IPv4 tuviera tanto éxito, vinculado al de Internet.

Además, IPv6 simplifica los encabezamientos de los paquetes de datos, con solamente 7 campos en lugar de 14. Así, los tratamientos por parte de los routers pueden ser más rápidos aumentando de este modo la velocidad. Las funcionalidades de traducción de direcciones (NAT - *Network Address Translation*) ya no son necesarias, lo que simplifica la arquitectura de red.

A nivel de seguridad, IPv6 incluye de forma nativa IPsec (*IP Security*). Este protocolo de seguridad se explicará más tarde en su totalidad.

Entre las características de esta nueva generación, podemos citar:

- Configuración Plug and Play, gracias a los mecanismos de autoconfiguración de las máquinas.
- Enrutamiento más eficaz, con una reducción de las tablas de transporte.
- Identificación de los flujos para el servicio integrado.
- Mecanismos estándar de seguridad.
- Movilidad.
- Número casi ilimitado de direcciones IP.
- Compatibilidad ascendente mantenida con IPv4, que garantiza una migración progresiva.

3. Estructura de una dirección IP

a. Categorías de direcciones

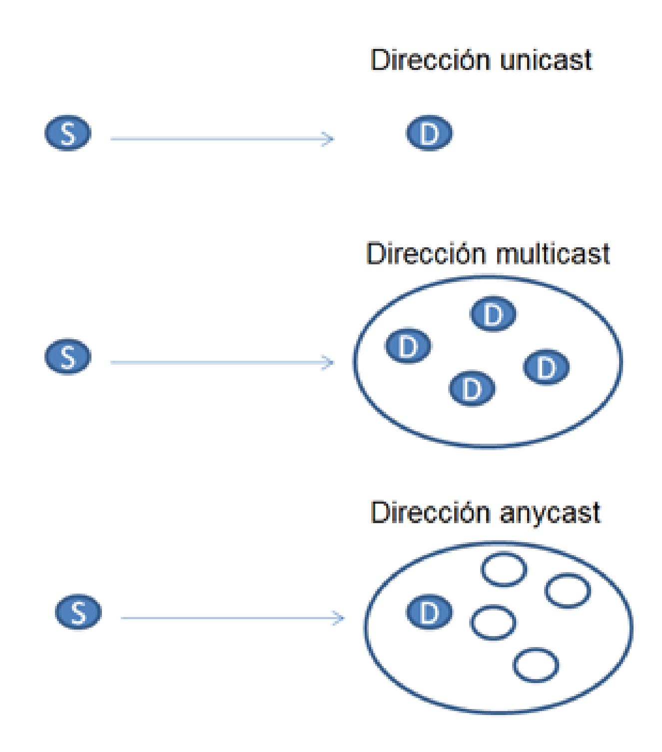
En IPv6, existen tres tipos de direcciones que corresponden a identificadores de 128 bits para interfaces o grupos de interfaces:

- *unicast*,
- *multicast*,
- *anycast*.

Una dirección *unicast* hace referencia a un identificador asociado a una sola interfaz, mientras que una dirección *multicast* hace referencia a un identificador de grupo cuyos miembros son interfaces: se va a asignar el identificador *multicast* a la interfaz.

El concepto de dirección *anycast* designa la interfaz «más cercana», miembro de un grupo, desde un punto de vista de la métrica utilizada (en el sentido de los protocolos de enrutamiento).

No existe el concepto de dirección de difusión (o broadcast) como se daba en IPv4. Las direcciones multicast sustituyen el broadcast definiendo además un ámbito de aplicación de esta dirección.



Tipos de direcciones IPv6

Por lo tanto, un paquete enviado a una dirección *unicast* se entregará únicamente a la interfaz identificada por esta dirección.

Un paquete enviado a una dirección *multicast* se transmitirá a todas las interfases identificadas con esta dirección.

Finalmente, un paquete enviado a una dirección *anycast* se transmitirá solamente a una de las interfaces (la más próxima) identificadas con esta dirección.

b. Ámbito de una dirección

Una dirección dispondrá de un ámbito más o menos importante según su categoría. Al contrario que IPv4, que separaba las direcciones públicas de las privadas, con IPv6 por una parte las direcciones van a tener una visibilidad mayor o menor y por otra parte una misma interfaz dispondrá de diferentes direcciones IP con una visibilidad diferente.

Una dirección *unicast* o *anycast* podrá disponer de los siguientes ámbitos:

- Ámbito **global** (ámbito mundial, Internet).
- Ámbito **local** (ámbito local, número limitado de sitios interconectados).
- Ámbito de **conexión local** (ámbito limitado a una subred no enrutada).

Teóricamente, una dirección *multicast* se podrá descomponer basándose en los siguientes niveles:

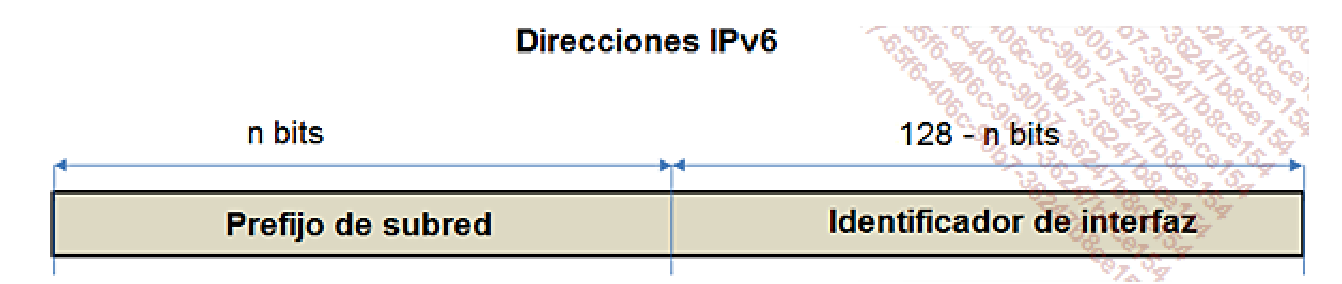
- Ámbito **global** (mundial).
- Ámbito **local en la empresa** (varios sitios de una misma empresa).
- Ámbito **local en el sitio** (sitio único).
- Ámbito **local del administrador** (el ámbito más pequeño que se puede configurar administrativamente con independencia de la topología física).
- Ámbito **local de la subred** (subred).
- Ámbito de **conexión local** (vecinos conectados en una misma conexión).
- Ámbito de **interfaz local** (interfaz).

El ámbito de la dirección se identificará por el prefijo de esta dirección, para las direcciones*unicast* y *anycast*, o por el campo **Ámbito** presente en el prefijo de una dirección *multicast*.

c. Dirección unicast

Las direcciones *unicast* pueden identificar un nodo de manera única (tarjeta de red o interfaz de router).

De manera general, las direcciones IPv6 *unicast* se presentan de la misma manera que las direcciones IPv4 sin clase CIDR (*Classless Inter Domain Routing*).



Hemos visto que estas direcciones pueden ser de ámbito global, de sitio o de conexión local.

También existen direcciones IPv6 que llevan encapsuladas direcciones IPv4.

Veremos un poco más tarde cómo funciona el establecimiento de la dirección en función de su ámbito y de su categoría.

d. Notación

Existen diferentes maneras de representar la direcciones IPv6.

La forma más usual es **xx : xx : xx : xx : xx : xx : xx : xx**.

donde «**xx**» corresponde a la representación hexadecimal de una palabra (2 bytes o 16 bits).

Ejemplos:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

2001:0:0:0:8:800:200C:417A

No es necesario escribir los ceros consecutivos de una palabra. Sin embargo, debe haber al menos una cifra por campo, excepto en el caso de utilización de la forma abreviada (ver más adelante).

Teniendo en cuenta los diferentes métodos de obtención de las direcciones, es habitual disponer de direcciones que tengan numerosos ceros consecutivos. Para facilitar la escritura de estas direcciones, una sintaxis especial, **la forma abreviada**, permite comprimir y simplificar esta escritura.

La utilización de «**::**» permite indicar uno o varios grupos de 16 bits de ceros.

Atención, este doble «**:**» solo debe aparecer una vez en una dirección. Se puede utilizar para comprimir los ceros iniciales o finales de la dirección.

La siguiente tabla permite ver las formas abreviadas que se pueden utilizar:

Ejemplo de dirección	Categoría	Forma abreviada
1080:0:0:0:8:800:200C:417A	una dirección*unicast*	1080::8:800:200C:417A
FF01:0:0:0:0:0:0:101	una dirección*multicast*	FF01::101
0:0:0:0:0:0:0:1	la dirección de bucle local	::1
0:0:0:0:0:0:0:0	una dirección no especificada	::

Existe una forma alternativa y a veces más práctica si se trabaja en un entorno mixto (IPv4 y v6):

xx : xx : xx : xx : xx : xx : a . b . c . d donde:

- «**xx**» representa la escritura hexadecimal de seis palabras (12 bytes) más significativas.
- «**a.b.c.d**» representa la dirección IPv4 en notación decimal punteada (4 bytes menos significativos).

A continuación ofrecemos algunos ejemplos:

Ejemplo de dirección	Forma abreviada
0:0:0:0:0:0:192.168.1.1	::192.168.1.1
0:0:0:0:0:FFFF:57.146.31.60	::FFFF:57.146.31.60

Finalmente, la **representación de los prefijos de las direcciones** sigue el mismo principio que la notación CIDR utilizada en IPv4:

Dirección-IP-v6 / longitud del prefijo, donde:

- «**Dirección-IP-v6**» se escribe siguiendo las reglas presentadas anteriormente.
- «**longitud-de-prefijo**» es un valor decimal que indica cuántos bits significativos (a la izquierda) forman parte del prefijo.

Así, el prefijo de 60 bits hexadecimal 200300000000ABC se escribe:

2003:0000:0000:ABC0:0000:0000:0000:0000/60

2003::ABC0:0:0:0:0/60

2003:0:0:ABC0::/60

Igualmente se puede escribir, como en IPv4, la dirección del nodo seguido del prefijo asociado a la red:

2003:0:0:ABC0:123:4567:89AB:CDEF/60

e. Identificador EUI-64

Concepto de identificador

Los identificadores de interfaz para las direcciones *unicast* en IPv6 permiten identificar las interfaces en una conexión dada. Este identificador debe ser único para una subred dada y lo puede ser también para un ámbito mayor, incluso global (Internet).

En algunos casos, el identificador se obtendrá directamente a partir de la dirección MAC (nivel 2) de la interfaz.

Este identificador se puede usar en el mismo nodo siempre que se utilice en interfaces diferentes conectadas en subredes diferentes.

Observe que no hay relación directa entre la singularidad del identificador de interfaz y la singularidad de direcciones IP. Por lo tanto, es posible crear una dirección *unicast* global disponiendo de un identificador de interfaz de ámbito no global, o crear una dirección local de sitio, con un identificador de ámbito global.

Además, cualquier dirección *unicast*, excepto aquellas que comienzan en binario por «**000**», deben tener un identificador de interfaz:

- de una longitud de 64 bits;
- construido según el formato EUI-64 modificado.

El identificador de interfaz, basado en el formato EUI-64 modificado, es de ámbito global, ya que está construido a partir de la dirección MAC. Por el contrario, el identificador es de ámbito local cuando no tiene ninguna información única o permanente para construir el identificador de interfaz (por ejemplo: conexión serie, terminaciones de túneles).

Construcción de un identificador EUI-64 modificado

Observe a continuación la dirección MAC asignada a la tarjeta de red y la dirección IPv6 correspondiente que se le ha autoasignado:

```
Administrador: Símbolo del sistema

Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : ULi PCI Fast Ethernet Controller
   Dirección física. . . . . . . . . . . . . : 00-18-F3-AE-07-4A
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Vínculo: dirección IPv6 local. . . : fe80::218:f3ff:feae:74a%4(Preferido)

   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.105(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Concesión obtenida. . . . . . . . . . . . : lunes, 04 de abril de 2011 7:20:5
3
   La concesión expira . . . . . . . . . . . : martes, 05 de abril de 2011 7:20:
52
   Puerta de enlace predeterminada . . . . . : 192.168.1.1
   Servidor DHCP . . . . . . . . . . . . . . : 192.168.1.1
   IAID DHCPv6 . . . . . . . . . . . . . . . : 234886031
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-15-04-5E-F2-00-13-8F-
7D-EE-13
   Servidores DNS. . . . . . . . . . . . . . : 192.168.1.1
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

En este caso, la dirección MAC es 00-18-F3-AE-07-4A.

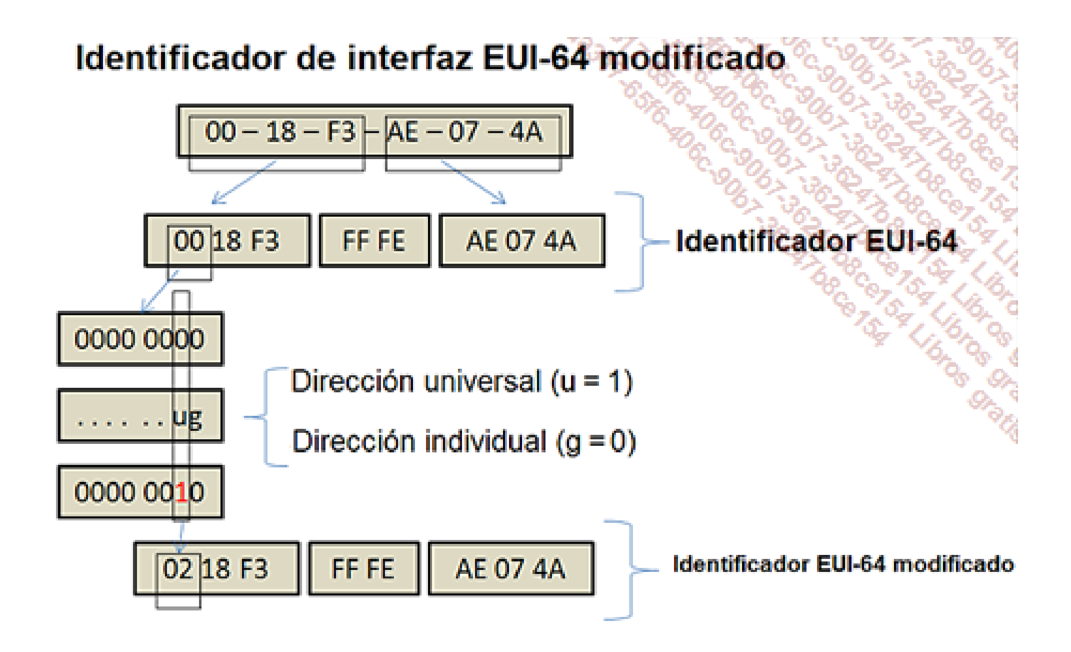
Los tres primeros bytes identifican al fabricante o OUI (*Organizationally Unique Identifier* - http://standards.ieee.org/regauth/oui/oui.txt) y los tres últimos identifican el hardware.

La dirección autoasignada es FE80::218:F3FF:FEAE:74A.

Observe que el "%4" define un índice para esta interfaz y define por tanto la asignación de esta misma dirección en otra interfaz de la misma máquina, a condición que se conecte en otra subred.

El identificador EUI-64 se construye a partir de la dirección MAC, insertando los dos bytes "**FF FE**" entre la OUI y la parte base de la dirección MAC.

El identificador EUI-64 modificado se obtiene poniendo a "1" el primer bit del byte significativo del OUI:



Finalmente encontramos:

FE80::218:F3FF:FEAE:74A

f. Direcciones reservadas

Existen diversas direcciones reservadas en IPv6.

El bucle local

La dirección de bucle local es

0000:0000:0000:0000:0000:0000:0000:0001

En escritura abreviada ::1

Esta dirección equivale a 127.0.0.1 en IPv4.

Cuando no se define ninguna dirección, se utiliza 0000:0000:0000:0000:0000: 0000:0000:0000. También se puede escribir 0:0:0:0:0:0:0:0, o incluso :: (doble «:»).

Las direcciones de transición IPv4 - IPv6

Para asegurar una transición entre las dos versiones, en ciertas circunstancias se pueden utilizar las direcciones IPv6 que se basan en direcciones IPv4.

Se puede utilizar una dirección IPv4 mapeada cuando se trate de comunicar, sea en IPv4, sea en IPv6, a partir de un equipo que disponga de doble pila de protocolo (IPv4/v6).

Esta dirección se puede representar utilizando una mezcla de las notaciones IPv6/v4.

Se escribirá en notación abreviada de la siguiente manera:

::FFFF:<dirección-ipv4-notación-decimal-punteada>

Por ejemplo, ::FFFF:192.168.1.200

Se podrá utilizar también la notación hexadecimal y escribir la dirección así:

::FFFF:C0A8:01C8

Donde 192 en base 10 (d) vale C0 en base 16 (h), o sea 192d = C0h, 168d = A8h, 1d = 1h y 200d = C8h.

En realidad es la dirección 0000:0000:0000:0000:0000:FFFF:C0A8:01C8.

0000	0000	0000	0000	0000	FFFF	C0A8	01C8

Las direcciones IPv4 compatibles sirven para encapsular IPv6 en IPv4 (por medio de un túnel). Estas direcciones se escriben poniendo los 96 bits significativos a 0 antes de cifrar la IPv4:

::<dirección-ipv4-notación-decimal-punteada>.

Ejemplo: **::192.168.1.200**

O **::C0A8 :01C8**

O sea

0000	0000	0000	0000	0000	0000	C0A8	01C8

Tenga en cuenta que la RFC 4291 trata estas direcciones como obsoletas. No se deben utilizar.

g. Descomposición de rangos para la IETF

Introducción

Los rangos de direcciones IPv6 (RFC 4291) se han descompuesto para IETF (*Internet Engineering Task Force*) de la siguiente manera:

Prefijo IPv6	Asignación	Referencia
0000::/8	Reservado	[RFC4291]
0100::/8	Reservado	[RFC4291]
0200::/7	Reservado (ej. NSAP)	[RFC4048]
0400::/6	Reservado (ej. IPX)	[RFC4291]
0800::/5	Reservado	[RFC4291]
1000::/4	Reservado	[RFC4291]
2000::/3	*Unicast* globales	[RFC4291]

4000::/3	Reservado	[RFC4291]
6000::/3	Reservado	[RFC4291]
8000::/3	Reservado	[RFC4291]
A000::/3	Reservado	[RFC4291]
C000::/3	Reservado	[RFC4291]
E000::/4	Reservado	[RFC4291]
F000::/5	Reservado	[RFC4291]
F800::/6	Reservado	[RFC4291]
FC00::/7	*Unicast* locales	[RFC4193]
FE00::/9	Reservado	[RFC4291]
FE80::/10	*Unicast* de conexión local	[RFC4291]
FEC0::/10	Obsoleto (*unicast* de sitio)	[RFC3879]
FF00::/8	*Multicast*	[RFC4291]

Se puede acceder a los documentos oficiales (RFC) en la siguiente URL:http://tools.ietf.org/html/

Así, cuando se retiran las direcciones reservadas, quedan las siguientes categorías:

- Direcciones *unicast* globales.
- Direcciones *unicast* locales.
- Direcciones *unicast* de conexión local.
- Direcciones *multicast*.

Tenga en cuenta que las direcciones *anycast* están incluidas en el rango de direcciones «*unicast* globales».

Explicaciones complementarias

El prefijo IPv6 se debe interpretar de la siguiente manera:

Por ejemplo, «**FC00::/7**» significa que los «7» bits significativos presentes en los 16 bits «FC00» se fijan.

- «**F**» se codifica en 4 bits en binario como «**1111**».
- «**C**» se codifica «**1100**».
- «**0**» se escribe «**0000**» en binario.

Por lo tanto:

- El byte escrito «**FC**» en hexadecimal vale «**1111 1100**» en binario.
- «**00**» en hexadecimal se escribe «**0000 0000**» en binario.

Una vez el prefijo hexadecimal se transcribe en binario, se identifican los n bits significativos (a la izquierda) después de «/» en la escritura del prefijo. Estos bits se deben fijar cuando se enumeran las posibles combinaciones.

FC00::/7	1111 110x.	xxxx xxxx

Así, FC00::/7 quiere decir que los bits significativos se pueden escribir con los valores «mínimo» y «máximo» siguientes:

- **1111 1100.0000 0000**
- y **1111 1101.1111 1111**

Finalmente, FC00::/7 expresa todas las direcciones cuyos prefijos están entre FC00 y FDFF.

Prefijo IPv6	Prefijo	Binario	Rango del prefijo
0000::/8	0000 0000.	xxxx xxxx	0000-00FF
0100::/8	0000 0001.	xxxx xxxx	0100-01FF
0200::/7	0000 001x.	xxxx xxxx	0200-03FF
0400::/6	0000 01xx.	xxxx xxxx	0400-07FF
0800::/5	0000 1xxx.	xxxx xxxx	0800-0FFF
1000::/4	0001 xxxx.	xxxx xxxx	1000-1FFF
2000::/3	001x xxxx.	xxxx xxxx	2000-3FFF
4000::/3	010x xxxx.	xxxx xxxx	4000-5FFF
6000::/3	011x xxxx.	xxxx xxxx	6000-7FFF
8000::/3	100x xxxx.	xxxx xxxx	8000-9FFF
A000::/3	101x xxxx.	xxxx xxxx	A000-BFFF
C000::/3	110x xxxx.	xxxx xxxx	C000-DFFF
E000::/4	1110 xxxx.	xxxx xxxx	E000-EFFF
F000::/5	1111 0xxx.	xxxx xxxx	F000-F7FF
F800::/6	1111 10xx.	xxxx xxxx	F800-FBFF
FC00::/7	1111 110x.	xxxx xxxx	FC00-FDFF
FE00::/9	1111 1110.	0xxx xxxx	FE00-FE7F
FE80::/10	1111 1110.	10xx xxxx	FE80-FEBF
FEC0::/10	1111 1110.	11xx xxxx	FEC0-FEFF
FF00::/8	1111 1111.	xxxx xxxx	FF00-FFFF

En resumen, a continuación se muestra la información que no hay que olvidar para identificar el tipo de una dirección IPv6:

Categoría de dirección	Prefijos	Mínimo	Máximo
Unicast global	2000::/3	2000	3FFF
Unicast local	FC00::/7	FC00	FDFF
Unicast de conexión local	FE80::/10	FE80	FEBF
Multicast	FF00::/8	FF00	FFFF

Otros protocolos de capa Internet

1. Internet Control error Message Protocol (ICMP)

ICMP es una especie de sub capa IP, que trabaja en paralelo con este protocolo. Su propósito es proporcionar el control y la interpretación de errores. De hecho, IP está sin conexión y no detecta anomalías en la red.

Los equipos IP utilizan el protocolo ICMP para especificar cierto número de eventos importantes en TCP, como:

- Descubrimiento de los routers.
- Medida de los tiempos de tránsito (PING - *Packet Internet Groper*).
- Redirección de las tramas...

Los datos del paquete IP son la cabecera y los datos ICMP. En la cabecera IP, el número de servicio es 1.

El mensaje ICMP se identifica por su tipo y su código. Hay diferentes mensajes, entre los que podemos citar:

Time Exceeded

Este mensaje indica que se ha sobrepasado el tiempo de espera para el destinatario. Se puede enviar si un paquete se pierde o si su TTL (en IPv4) es 0.

En este caso, el Tipo se informa a 11 y el código a 0 o 1.

```
D:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

D:\Users\Juanki>ping 12.12.12.12

Haciendo ping a 12.12.12.12 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 12.12.12.12:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

D:\Users\Juanki>
```

Ejemplo de mensaje «Time Exceeded» o «tiempo de espera agotado para esta solicitud»

Destination Unreachable

Este mensaje avisa que no se ha podido enrutar el paquete hacia su destino. Indica, por ejemplo, un problema en una ruta para llegar a una subred.

```
D:\Windows\system32\cmd.exe

D:\Users\Juanki>ping 192.168.1.200

Haciendo ping a 192.168.1.200 con 32 bytes de datos:
Respuesta desde 192.168.1.11: Host de destino inaccesible.
Respuesta desde 192.168.1.11: Host de destino inaccesible.
Respuesta desde 192.168.1.11: Host de destino inaccesible.
Respuesta desde 192.168.1.11: Host de destino inaccesible.

Estadísticas de ping para 192.168.1.200:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),

D:\Users\Juanki>
```

Ejemplo de mensaje «Destination Unreachable» o «Host de destino inaccesible»

Redirect

Este mensaje indica al emisor que existe un camino mejor hacia el destino.

Echo request y Echo Reply

Estos dos mensajes permiten probar si un nodo se puede comunicar con otro (petición de eco y respuesta al eco).

El comando Ping las utiliza.

```
D:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

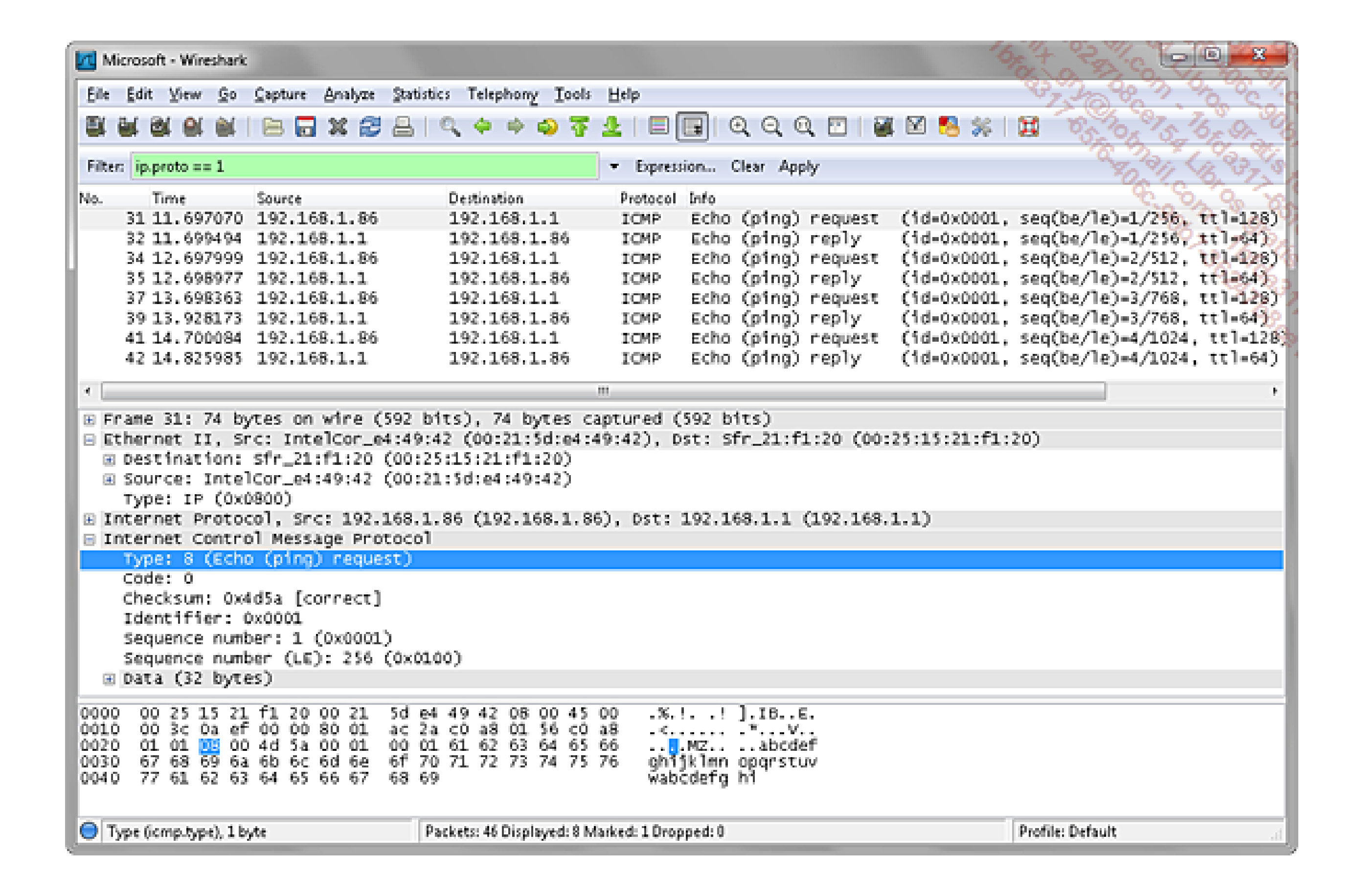
D:\Users\Juanki>ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 1ms, Media = 1ms

D:\Users\Juanki>
```

El tipo y el código de Echo Request se informan a 0. La respuesta positiva se indica con un mensaje de tipo 8 y el código se queda a 0.



Esta trama se ha generado a partir de un comando ping 192.168.1.1 repetido cuatro veces desde un ordenador cuya dirección IP es 192.168.1.86.

2. Internet Group Management Protocol (IGMP)

Este protocolo de la capa de Red permite a un equipo añadirse o salir de un grupo multidifusión (*multicast*).

La cabecera IGMP se encapsula dentro de un paquete IP y tiene poca información, como, por ejemplo, un tipo que determina las diferentes acciones de identificación sobre un grupo, la información de pertenencia y de salida del grupo. También contiene la dirección del grupo al que se dirige la información.

3. Address Resolution Protocol (ARP) y Reverse Address Resolution Protocol (RARP)

El objetivo del protocolo ARP es determinar la dirección MAC (dirección física) de un nodo a partir de su dirección IP (dirección lógica), en IPv4.

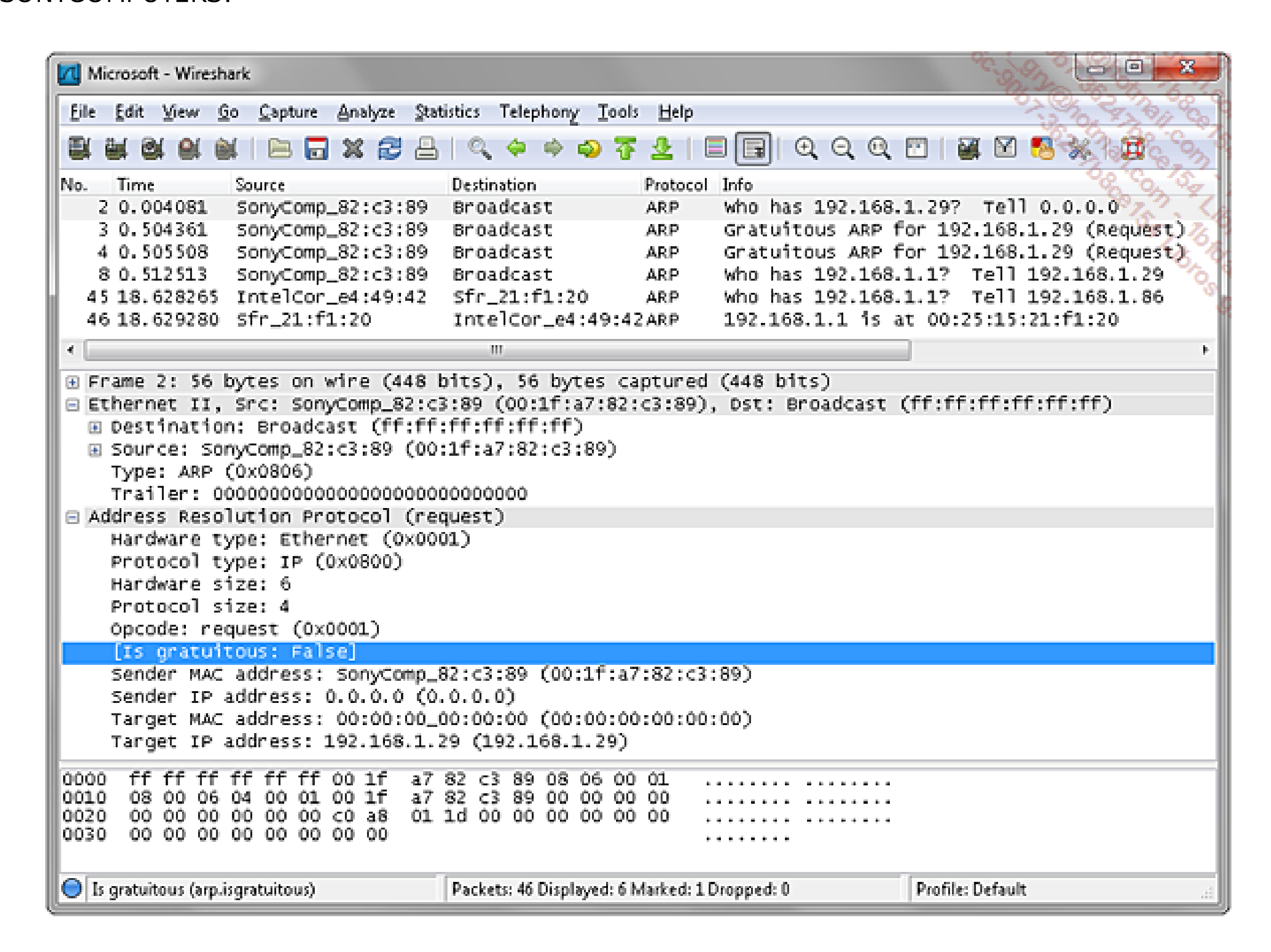
Se emite una difusión para encontrar una información concreta. Como se ha visto anteriormente, ARP administra una tabla de correspondencia (caché) para almacenar las relaciones. Esta resolución es necesaria para poder dirigir la trama al dispositivo adecuado en la red IP local.

ARP se adapta a los protocolos de capas bajas utilizados, incorporando los mensajes en estas tramas.

RARP (*Reverse ARP*) es una resolución inversa.

A continuación se observa el resumen de capturas de tramas ARP. El ordenador con dirección MAC 00:1F:A7:82:C3:89 busca al ordenador cuya dirección IP es 192.168.1.29. Observe que los tres primeros bytes de la dirección MAC (OUI) se sustituyen por el nombre del fabricante

SONYCOMPUTERS:



Tenga en cuenta que, al contrario que en otros protocolos, ARP no es un protocolo basado en IP. Por el contrario, lo sustituye y se encapsula directamente en la capa física (por ejemplo, Ethernet).

4. IP Security (IPsec)

IPsec está diseñado para asegurar diferentes tipos de seguridad:

- Confidencialidad y protección contra el análisis del tráfico, a través del cifrado.
- Autenticidad de los datos y control de acceso a través de la autentificación mutua de los dos extremos de la comunicación, la firma, así como cálculos de integridad.
- Protección contra la inyección de paquetes.

La repetición (*replay*) es una técnica que puede utilizar un intruso y que consiste en reenviar paquetes capturados durante una comunicación de red. El servidor recibe así la misma información repetida y sistemáticamente tiene que volver a procesarla y puede malinterpretar estos paquetes idénticos. Para evitar esta relectura, esta función antirrepetición añade un número de secuencia a la información. Así, el servidor es capaz de distinguir los paquetes que ya ha recibido y no volverá a tratarlos.

IPsec distingue dos niveles de protección a través de dos protocolos:

- *Authentication Header* (AH), que solo se ocupa de la autentificación, el control de integridad y el antirrepetición.

- *Encapsulating Security Payload* (ESP), que agrega la función de confidencialidad.

AH y ESP se pueden utilizar de manera conjunta o por separado, en función del nivel de protección deseado.

El primer nivel, o modo de transporte, protege una comunicación específica entre dos entidades. Así, por ejemplo, los paquetes de comunicación de una aplicación, correspondiente a un puerto TCP dado, pueden ser seguras, sin que influya en el conjunto del tráfico.

El modo túnel se utiliza para proteger todas las comunicaciones entre dos entidades.

5. Lista de los números de protocolos de la capa Internet

Estos números de protocolo se pueden visualizar en parte en el archivo «Protocolo» que está en la misma carpeta que el archivo «Servicios» en Windows y «protocols» y «services» en Linux.

A continuación puede ver los principales números:

N.° protocolo IP	**Nombre del protocolo**
0	*Internet Protocol* (IP)
1	*Internet Control error Message Protocol* (ICMP), utilizado principalmente por ping
6	*Transmission Control Protocol* (TCP)
17	*User Datagram Protocol* (UDP)
47	*Generic Routing Encapsulation* (GRE), utilizado por PPTP
50	*Encapsulating Security Payload* (ESP), utilizado por IPsec
51	*Authentication Header* (AH), utilizado por IPsec

Voz sobre IP (VoIP)

1. Principios

Las redes informáticas no solo transportan datos de texto. Hoy en día se digitalizan sonidos, fotos y vídeos y se transmiten como datos informáticos en los paquetes IP.

La aplicación del transporte de las comunicaciones orales digitalizadas, voz sobre IP (VoIP -*Voice over IP*), va encontrando su lugar tanto en las empresas como en las comunicaciones entre particulares.

En concreto, las aplicaciones de telefonía que utilizan TCP/IP se denominan ToIP (*Telephony over IP*).

La fusión entre las dos redes, telefónica e informática, revierte en beneficio de esta última si tiene la calidad suficiente. De hecho, la transmisión de una conversación telefónica no sufre ningún corte ni retardo que pueda alterarla. Se debe implementar la calidad del servicio (QoS -*Quality of Service*) para dar prioridad a estos paquetes y se debe disponer de una velocidad suficiente.

Con la mejora de la calidad de las redes locales y remotas y la adopción de la calidad del servicio, hoy en día son frecuentes estos servicios.

2. Algunas definiciones importantes

Antes de describir más detalladamente la VoIP, recordemos algunos términos de la telefonía analógica.

Centralita telefónica

Este término ambiguo puede designar indiferentemente la operadora que va a descolgar, el aparato multifunción a partir del cual la operadora va a realizar las operaciones, el número principal de la empresa a la que se llama o incluso el desvío de la llamada para el acceso al puesto de la persona con la que se quiere hablar.

Se pueden utilizar diversas funcionalidades por medio de una centralita telefónica. Varían en función del grado de sofisticación del equipo que se emplea.



Centralita telefónica

Entre las principales funcionalidades que ofrece una centralita, encontramos la gestión de un número único, que corresponde a la empresa, y a partir del cual se distribuyen las llamadas a los diferentes puestos de los empleados.

Igualmente encontramos:

- La gestión de llamadas en espera.
- La gestión de los mensajes de voz.
- La identificación de llamada.
- La gestión de la numeración abreviada.
- La marcación directa de extensiones.
- La gestión de estadísticas y de datos de refacturación (si fuera el caso).

Cuando la centralita telefónica se convierte en un conmutador, se hablará de PABX o de IPBX(ver más abajo), donde el objetivo principal es la comunicación entre la persona que llama y la que es llamada, dentro de una misma empresa, o desde una empresa al exterior.

En telefonía analógica, el **PABX** o *Private Automatic Branch eXchange* es un conmutador telefónico privado que permite conectar los puestos telefónicos de una red interna de una empresa con los de la red telefónica pública (líneas externas).

Un IPBX o PBX-IP es un servidor de aplicaciones que puede realizar la misma función que el PABX, pero en un entorno de VoIP.

Hoy en día, algunos IPBX pueden realizar igualmente la misma función que un PABX.



Ejemplo de IPBX - PABX: centralita telefónica Aastra/Ericsson

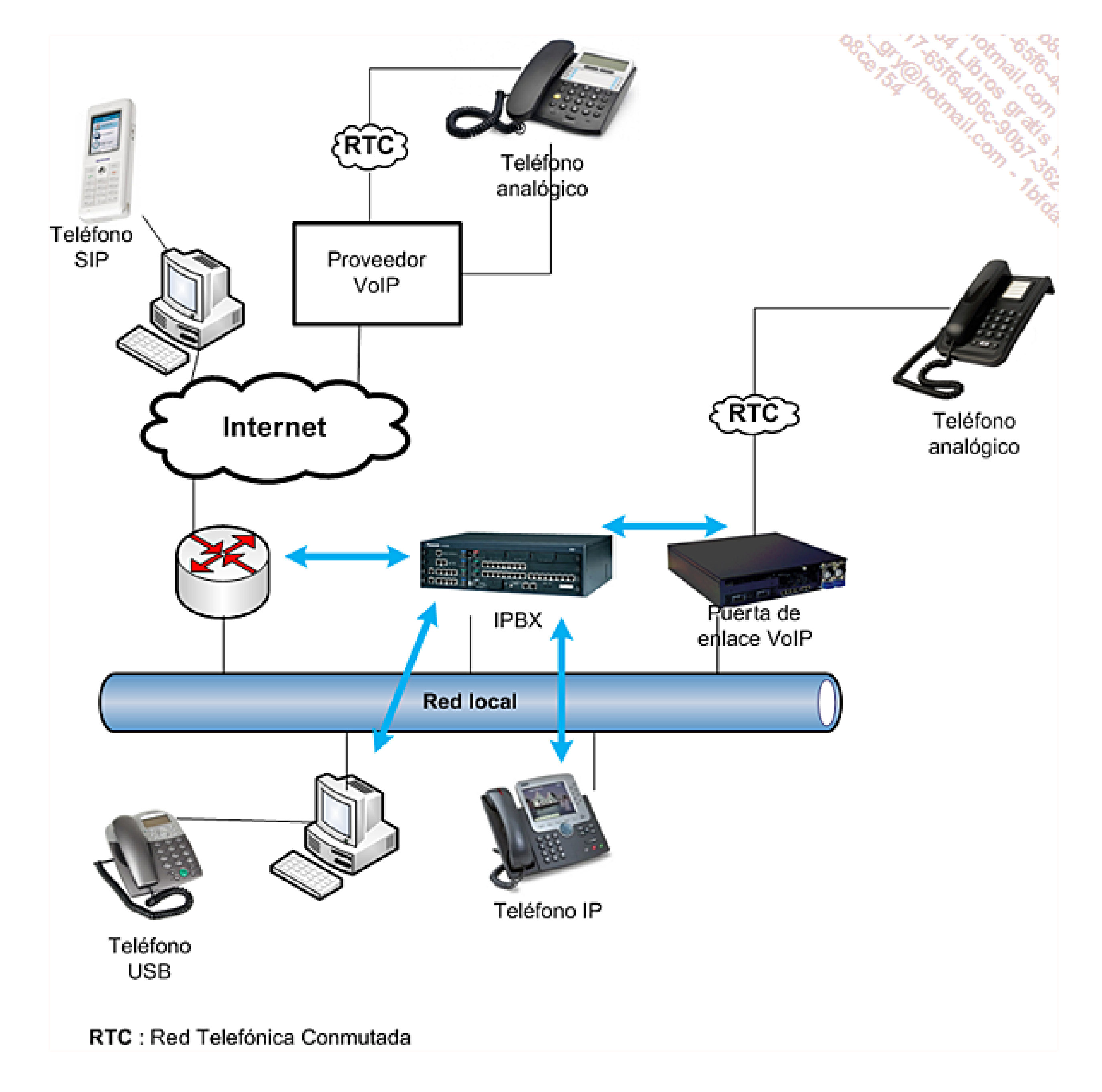
3. Ventajas

La primera ventaja de la voz sobre IP es que permite la unificación en la empresa de las dos redes, telefónica e informática. Se puede ver una importante reducción de costes.

Además, si ToIP se utiliza en las comunicaciones telefónicas externas, no es necesario movilizar una línea de conmutación de circuito. Como la comunicación se puede hacer por Internet por conmutación de paquetes, puede ser objeto de una tarifa plana, en función de las velocidades de subida y bajada asignadas. El coste no es proporcional al doble criterio de duración y distancia de la comunicación.

En términos aplicativos, se facilita el desarrollo del software que utiliza la voz (mensajería unificada, videoconferencia...).

De este modo, el entorno vinculado a la telefonía ha cambiado mucho. Se unen diferentes tecnologías que deben coexistir:



Integración de la telefonía IP en la red de una empresa

- En Internet hay disponibles numerosos proveedores de VoIP. En la URLhttp://www.voipproviderslist.com/ puede encontrar una lista de estos proveedores.

- En algunas configuraciones, los equipos de trabajo están conectados directamente al teléfono IP que actúa como conmutador de nivel 2.

Para terminar, el transporte de la voz sobre IP utiliza estándares abiertos e interoperables. La sostenibilidad de este sistema parece, pues, garantizada. Por el contrario, no se puede olvidar que el transporte tiene que ser seguro. Algunas comunicaciones deberían cifrarse para evitar que se pirateen, como cualquier dato informático confidencial.

4. Funcionamiento

a. El protocolo H323

La serie de protocolos H32x de la Unión International de Telecomunicaciones (UIT) está dirigida a estandarizar las diferentes funciones de videoconferencia, combinando audio, vídeo y transferencia de archivos. En 1996 nace la voz por IP, por medio de H323, capaz de basarse en diferentes protocolos de comunicación, códecs de audio y códecs de vídeo.

Su uso es independiente del tamaño de la red. Su utilización es posible, tanto en redes locales, en las que el ancho de banda es grande, como en Internet, que se caracteriza por velocidades menores y mayores retrasos en la transmisión.

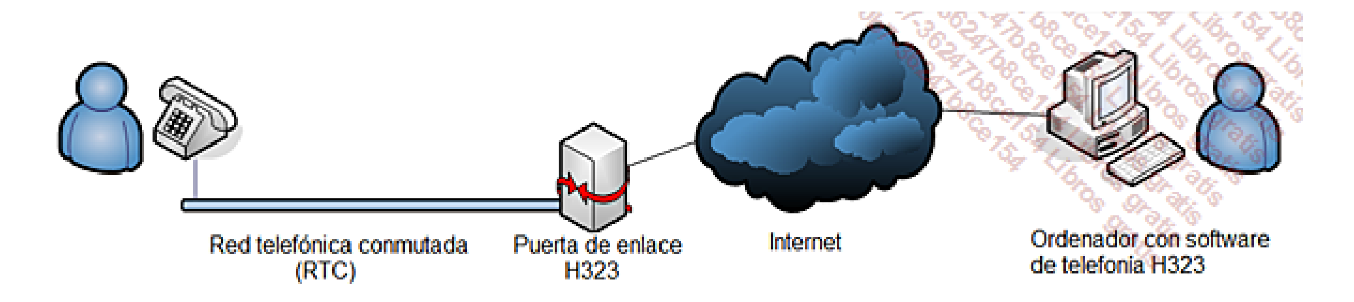
b. Los elementos terminales

Las dos partes de la comunicación telefónica pueden utilizar diferentes terminales que cumplan la norma H323.

Son preferibles los terminales digitales, como un PC o un teléfono diseñado para la voz por IP. Cada uno está identificado por su dirección IP. Si una de las partes utiliza un teléfono analógico, la comunicación debe pasar por una puerta de enlace.

Por ejemplo, si los dos comunicantes utilizan un PC, basta con un software de telefonía que implemente el protocolo H323 para dirigir los paquetes, gracias a la dirección IP de cada equipo. Todo el tráfico transita por la red local o Internet. El principio es el mismo si los equipos telefónicos son digitales, como en una comunicación en voz por IP en la empresa. Naturalmente, en este caso, se asocia un número de teléfono a la dirección IP del terminal.

Por el contrario, si uno de los comunicantes, o los dos, utilizan un teléfono clásico, una puerta de enlace tiene que hacer la conexión entre el transporte informático y el telefónico, asegurando así la interconexión entre los dos tipos de redes.



c. Las aplicaciones

Muchos proveedores de acceso a Internet, a través de su oferta tres en uno, ofrecen la telefonía personal por VoIP (o ToIP). Para esto, deben implementar su propia puerta de enlace con objeto de interconectar al abonado con la red telefónica de Telefónica. Este abonado puede tener un número estándar, con total transparencia. Incluso, cuando se quiera comunicar con otro abonado, le basta con marcar el número correspondiente.

En casa del abonado, un router/módem conectado a la toma de teléfono tiene un software de digitalización de la voz para transportarla en paquetes IP. Para reconstruir la voz analógica que el teléfono entiende, se realiza la operación inversa.

Las aplicaciones de VoIP/ToIP en empresas son más complejas. No solamente agrupan en la red informática local los dos tipos de comunicación, sino que además ofrecen numerosas funcionalidades complementarias (buzones de voz, directorios...). Se habla de mensajería unificada. Las llamadas telefónicas externas a través de Internet son una excepción porque no siempre se implementan.

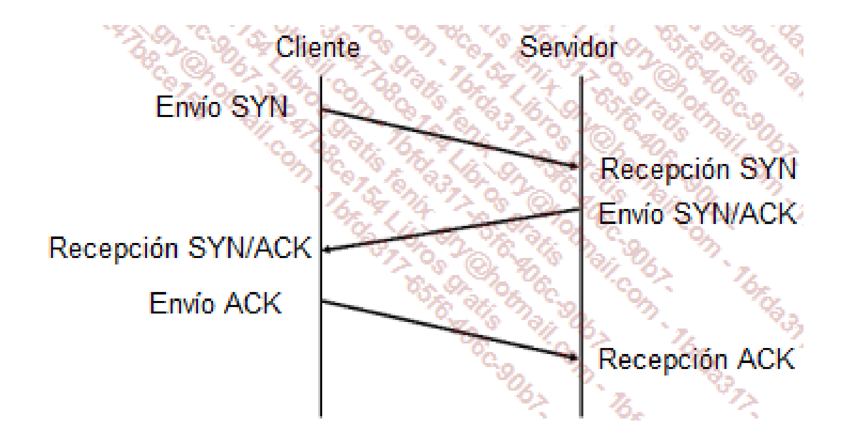
Se pueden instalar aplicaciones de telefonía en VoIP en los ordenadores. Permiten una comunicación gratuita a través de Internet. Actualmente, el software más popular para ello es Skype. El servicio de puerta de enlace, para poder llamar a un equipo telefónico clásico, es de

pago.

Protocolos de transporte TCP y UDP

1. Transmission Control Protocol (TCP)

Este protocolo está orientado a la conexión. Inicialmente se abre una sesión entre el cliente y el servidor.



Establecimiento de una sesión TCP

Después de la apertura de sesión, TCP completa las IP que faltan asegurando así la fiabilidad del servicio. Para ello, un acuse de recibo (ACK - *Acknowledge*) responde sistemáticamente a los paquetes.

TCP asegura la llegada correcta de toda la información. En contrapartida, esta función puede ralentizar la comunicación.

Con objeto de acelerar un poco el sistema y hacer que el emisor no espere recibir el acuse de recibo para seguir enviando información, se utiliza el concepto de ventana corredera. El emisor envía una batería de información y trata los acuses de recibo a medida que le van llegando sin parar de enviar información.

Después de la comunicación, la conexión normalmente termina con un mensaje de fin de envío (END) y el acuse de recibo correspondiente. Se puede avisar de una desconexión repentina por cualquiera de las dos partes con una señal de reinicialización (RST - *Reset*).

2. User Datagram Protocol (UDP)

Al contrario que TCP, UDP no asegura la conexión y pasa el proceso de comprobación a la capa superior (aplicación). Funciona en modo desconectado, lo que permite ganar velocidad en grandes transmisiones como vídeos y sonidos.

Capa de aplicación TCP/IP

1. Servicios de mensajería

a. Simple Mail Transfer Protocol (SMTP)

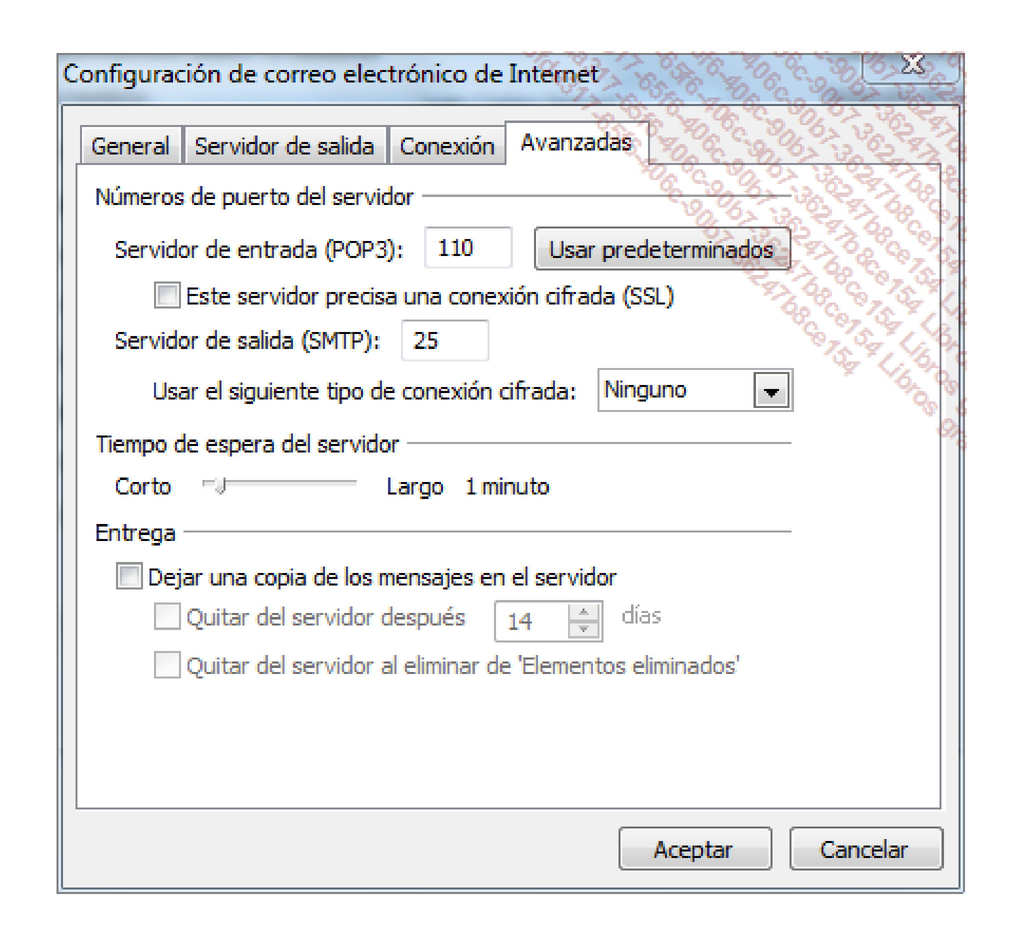
SMTP es un protocolo de transferencia simple que se utiliza en mensajería electrónica. Se basa en TCP e IP y no integra ninguna interfaz de usuario.

El objetivo de SMTP es transmitir mensajes (e-mail) hasta el buzón de correo del destinatario.

Este protocolo utiliza equipos distintos y nombrados según su función:

- MUA (*Mail User Agent*), cliente de mensajería.
- MTA (*Mail Transfer Agent*), transmisor de correo.
- MDA (*Mail Delivery Agent*), servicio de entrega de correo en los buzones de los destinatarios.

Este protocolo utiliza el puerto TCP 25 en el lado del servidor. La RFC 5321 describe el funcionamiento de este protocolo.



Para el envío de un mensaje por SMTP, se deben identificar un emisor y un destinatario. Para ello, deben tener una dirección formada por la referencia del buzón a la izquierda del signo @, y por un nombre de dominio a la derecha.

El mensaje se divide en tres partes:

- Un sobre, que los agentes utilizan para el enrutamiento.
- Una cabecera, que incluye las direcciones y el objeto.
- El cuerpo, que contiene el mensaje.

b. Post Office Protocol 3 (POP3)

Al contrario que SMTP, que tiene el papel de transporte, POP se dedica específicamente a la publicación y al acceso remoto a un servidor de correo.

El servidor POP se comunica con el agente usuario (*User Agent*), por ejemplo Mozilla Thunderbird, a través de una conexión síncrona. El servidor transfiere al cliente los mensajes, y después los elimina a petición del cliente.

Normalmente, el servidor solo conserva los mensajes que no se han transferido al cliente.

 POP 3 se define en la RFC 1939 y utiliza el puerto TCP 110 y el 995 en modo seguro.

Con POP, el cliente tiene que establecer una conexión previa con el servidor utilizando un usuario y una contraseña. Por supuesto, es el cliente de correo el que se encarga de ello. La sesión se cerrará con el comando *quit*. Una vez se ha establecido la conexión, el servidor bloquea el buzón del usuario y entra en fase de transacción.

Por defecto, con POP el nombre y la contraseña se transmiten sin cifrar. Algunos servidores POP implementan el algoritmo MD5 (*Message Digest 5*, RFC 1321) para proteger la contraseña enviada.

Configuración POP para Mozilla Thunderbird

c. Internet Message Access Protocol (IMAP)

IMAP permite almacenar y conservar en el servidor los correos electrónicos (e-mails), en lugar de descargarlos sistemáticamente en el cliente.

De hecho, el cliente IMAP se conforma con visualizar de forma remota las cabeceras de los mensajes y permite elegir cuáles se descargan finalmente.

IMAP tiene una gran ventaja sobre POP3 y se presentó como su sucesor. De hecho, a veces se hablaba de IMAP4 para indicar este hecho. El modo de funcionamiento de IMAP podría haber sido una ventaja crucial si la descarga de mensajes se hubiera continuado haciendo por líneas analógicas lentas, que facturaban en función del tiempo.

El crecimiento de las conexiones de banda ancha fue un primer freno para el uso de IMAP en lugar de POP3. Además, la generalización de la consulta de los mensajes directamente en los sitios Web (*webmail*) ha anulado las ventajas de las funcionalidades complementarias que podían ser interesantes.

Sin embargo, desde hace algunos años, IMAP ha conseguido avanzar y la mayor parte de los operadores lo ofrece y está incluido en numerosas herramientas colaborativas.

Hay numerosos comandos disponibles en IMAP. Permiten gestionar los buzones, los mensajes, efectuar búsquedas, transferencias selectivas... Con IMAP, también es posible compartir un mismo buzón de correo entre diferentes personas.

2. Servicios de transferencia de archivos

a. HyperText Transfer Protocol (HTTP)

HTTP es, sobre todo, un protocolo de transferencia de archivos. *HyperText Markup Language*(HTML) se utiliza para formatear y visualizar. Los archivos transmitidos al cliente los interpreta un software navegador (*browser*).

El protocolo HTTP es utilizado por un servidor Web, que almacena la información en forma de páginas de texto (HTML), imágenes, vídeos, sonidos… Cada entidad corresponde a un archivo, dentro de una jerarquía.

La versión de HTML que actualmente está en desarrollo es la versión 5, que nació en 2006. La última versión completa, la 4.01, data de 1999.

Sin embargo, la mayor parte de los navegadores de Internet, en sus últimas versiones, incorporan las novedades ofrecidas por esta versión del protocolo (Internet Explorer, Chrome, Firefox, Safari u Opera).

La URL http://html5test.com/ permite probar las funcionalidades HTML5 que soporta su navegador

HTML5 proviene de la colaboración entre el W3C (*World Wide Web Consortium*), que sobre todo ha trabajado en XHTML 2.0, y de WHATWG (*Web Hypertext Application Technology Group*), que se centró en los formularios y aplicaciones web.

Se han enunciado algunas nuevas reglas para esta nueva versión:

- Las nuevas funcionalidades deben basarse en HTML, CSS (*Cascading Style Sheet* u hojas de estilo en cascada), DOM (*Document Object Model*) y JavaScript.
- Se debe reducir al máximo la utilización de componentes externos (p. ej., Plugin Flash).
- Debe haber un perfecto control de errores.
- Numerosas etiquetas complementarias reemplazan a scripts.

- HTML5 debe ser independiente de los dispositivos.
- Los procesos de desarrollo deben ser accesibles al público.

En HTML5 solo hay una declaración <!DOCTYPE>.

De este modo, el documento HTML5 más pequeño posible se parecerá a este:

```
<!DOCTYPE html>
<html>
<head>
<title>Título del documento</title>
</head>

<body>
El contenido del documento...
</body>

</html>
```

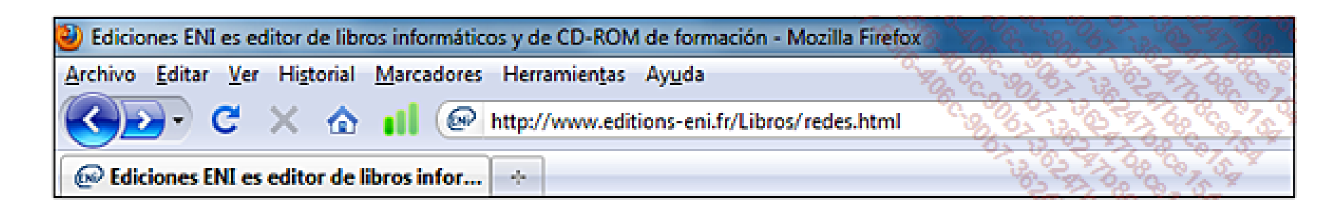
Entre las nuevas funcionalidades de HTML5, se encuentran:

- El elemento `<canvas>` para el diseño 2D.
- Los elementos `<audio>` y `<video>` para las funcionalidades multimedia.
- La implementación del almacenamiento local.
- Nuevos elementos que definen nuevos contenidos, como `<article>`, `<section>`, `<nav>` o `<footer>`.

<nav> permite definir vínculos de navegación. <footer> es la firma o el pie de página de un documento.

- Nuevos formularios, como *calendar*, *date*, *time*, *email*, *search* o *url*.

Para visualizar esta información, se utilizan las URL (*Uniform Resource Locator*). Una URL requiere, en primer lugar, el protocolo (http://) y a continuación el alias del servidor Web y la referencia de la entidad.



Llamada a una URL en un navegador

Por ejemplo, un navegador puede mostrar la página «redes.html» del directorio «Libros» llamando a la URL http://www.editions-eni.fr/libros/redes.html, que está gestionada por el servidor www.eni.fr.

Para formular las comunicaciones entre clientes y servidores, el protocolo HTTP utiliza comandos, llamados métodos, en el puerto TCP 80. Estos métodos ofrecen diferentes funciones, como la llamada a páginas (*get*), el envío de formularios (*post*)...

El protocolo que se utiliza actualmente es HTTP 1.1.

De forma predeterminada, el texto transmitido entre un cliente y un servidor se realiza sin cifrar. De esta manera es perfectamente legible por cualquiera que intercepte la conversación. Para solucionar este defecto, la versión segura del protocolo, HTTPS (TCP 443), cifra la comunicación y convierte la información en confidencial.

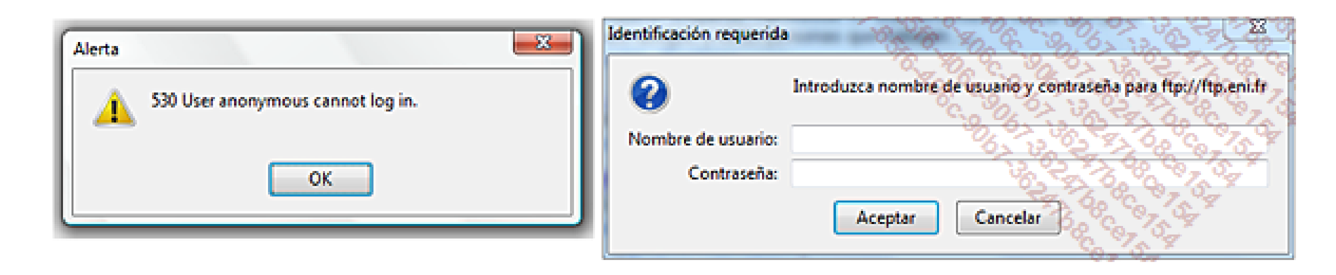
El protocolo HTTPS también se denomina SSL (*Secure Socket Layer*). Su versión estándar, que se puede usar con otros protocolos, es TLS (*Transport Layer Security*). Esta denominación muestra una voluntad más general de cifrar la comunicación.

Aviso de IE9 de conexión a un sitio seguro (diálogo SSL)

b. File Transfer Protocol (FTP) y Trivial FTP (TFTP)

FTP es un protocolo de transferencia de archivos basado en un método fiable e implementado en TCP. La principal ventaja de FTP es que se puede utilizar entre sistemas operativos diferentes, que se basan en sistemas de archivos heterogéneos.

El protocolo FTP ofrece dos tipos de acceso. El primero es una conexión anónima, con el identificador predeterminado anónimo. Este modo es similar a la conexión HTTP «clásica». Por el contrario, podemos querer que la descarga de archivos en un sentido o en otro sea segura. Por lo tanto, es posible solicitar la autentificación de una cuenta de usuario conocida.



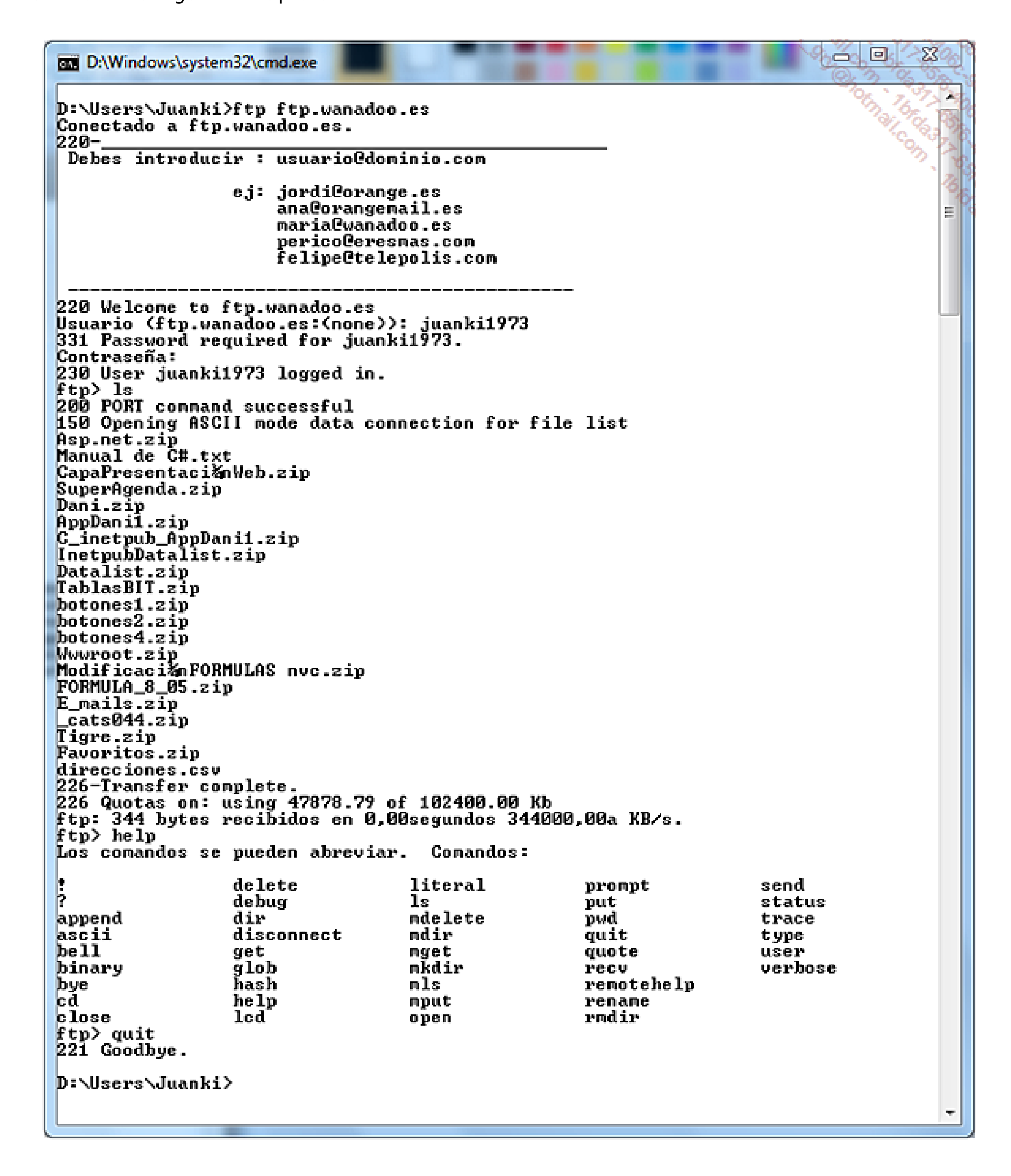
Solicitud de autentificación y mensaje que detalla la prohibición de uso anónimo

El usuario podrá entonces, mediante la utilización de comandos propios de FTP, mover archivos de un directorio a otro (según los permisos de los que el usuario disponga en cada sistema).

Hay dos tipos de clientes FTP. El primero es gráfico y la mayoría de veces tiene la forma de un

navegador, que ofrece funciones como tal, como Internet Explorer o Firefox.

Para los puristas en Windows o Linux, está disponible el cliente de línea de comandos, como se muestra en la siguiente captura:

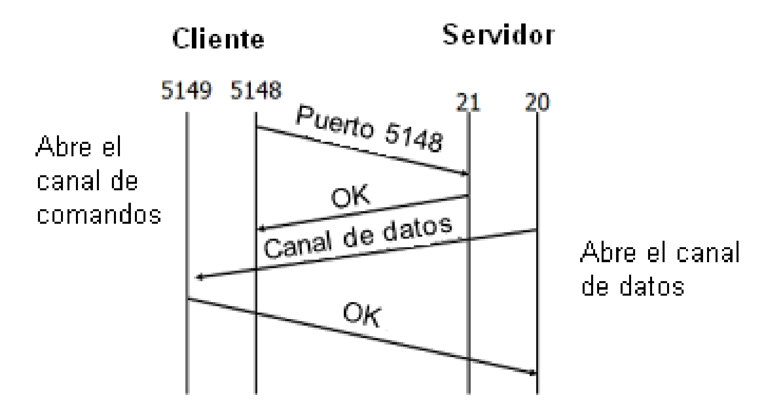


Ejemplo del entorno interactivo FTP

El protocolo FTP es peculiar, ya que utiliza dos conexiones separadas para su uso:

- Un canal de comandos/control en el puerto 21 (lado servidor).
- Un canal de datos, en el puerto 20 (lado servidor).

Además, este protocolo ofrece dos modos. El primero, activo, parece un diálogo de tipo cliente/servidor, pero con la utilización de 2 canales (comandos y datos). En el siguiente esquema se puede ver su funcionamiento.



El segundo modo, pasivo, se diseñó para la transferencia de archivos entre servidores. En este caso, el canal de datos no es en el puerto 20, sino en un puerto aleatorio.

Trivial FTP (TFTP) permite descargar más rápidamente la información pero sin garantizar su integridad. Su falta de fiabilidad se basa en el hecho de que utiliza el protocolo UDP en lugar de TCP para el transporte. Este protocolo se utiliza en redes locales de diseño reciente, que podemos considerar en principio más fiables.

Se utilizará igualmente TFTP para realizar copias de seguridad de configuraciones de conmutadores o routers. Para hacer la copia de seguridad diaria de un router CISCO Router1 en un servidor TFTP, cuya dirección es 10.1.2.100, se utilizará el siguiente comando:

```
Router1#copy running-config tftp:
Address or name of remote host []? 10.1.2.100
Destination filename [router1-confg]?
Copia_de_seguridad_de_mi_router!!
1030 bytes copied in 2.489 secs (395 bytes/sec)
Router1#
```

De igual modo, para restaurar esta copia de seguridad en otro router, Router2, se puede utilizar un comando parecido:

```
Router2#copy tftp: running-config
Address or name of remote host []? 10.1.2.100
Source filename []? Copia_de_seguridad_de_mi_router
Destination filename [startup-config]?
Accessing tftp://10.1.2.100/Copia_de_seguridad_de_mi_router...
Loading Copia_de_seguridad_de_mi_router from 10.1.2.100
 (via FastEthernet0/0): !
 [OK - 1030 bytes]
1030 bytes copied in 9.612 secs (107 bytes/sec)
Router2#
```

c. Network File System (NFS)

Desarrollado por SUN en 1985, NFS es un sistema de archivos distribuido para entornos heterogéneos. Permite a los usuarios de ordenadores y sistemas operativos diferentes acceder a un sistema de archivos remoto, sin tener que aprender nuevos comandos.

NFS fue el primer intercambio de archivos verdaderamente operativo y constituyó un complemento indispensable del entorno de estaciones de trabajo que ofrecía SUN. La popularidad de su sistema operativo SOLARIS permitió contribuir al éxito de NFS.

A lo largo del tiempo se han creado diferentes versiones de NFS:

NFSv2 y v3 se basan en las llamadas a procedimientos remotos o RPC (*Remote Procedure Call*) y se definen respectivamente en las RFC 1094 y 1813.

La versión 2 es más antigua y está ampliamente extendida.

La versión 3 mejora un poco la gestión de errores y permite tratar bloques de tamaño variable, pero no es completamente compatible con la v2.

La versión 4 ya no utiliza los RPC que se basan en puertos aleatorios y que acarrean problemas de seguridad cuando se utilizan cortafuegos entre clientes y servidores.

Esta última versión, definida en la RFC 3530, implementa igualmente kerberos para la autenticación y permite gestionar listas de control de acceso (ACL o *Access Control List*) para permitir definir autorizaciones basándose en grupos de usuarios.

A pesar de su antigüedad, este protocolo de gestión de archivos en red está presente hoy en día en las empresas, en particular al lado de CIFS (*Common Internet File System* o sistema de archivos Microsoft).

Los NAS (*Network Attached Storage*) ofrecen NFS. Aparece como rol de servicio en Windows Server 2008 y 2012. En Windows 7 hay también un cliente NFS como componente opcional que se puede activar.

3. Servicios de administración y de gestión de red

a. Domain Name System (DNS)

Introducción

El objetivo del sistema de nombres de dominio es ofrecer una resolución basada en nombres jerárquicos y distribuidos para los huéspedes IP conectados a la red.

El sistema de nombres de dominio existe desde 1983, año en que fue creado por Paul Mockapertis (RFC 882 y 883); remplazó históricamente la gestión de un archivo *hosts* que se utilizaba al principio en Internet y que era mantenido por el *Network Information Center* del*Stanford Research Institute* (SRI).

La norma correspondiente a DNS se publicó finalmente en 1987 (RFC 1034 y 1035).

Al principio el sistema permitía solamente resolver nombres en direcciones IP, así como direcciones IP en nombres.

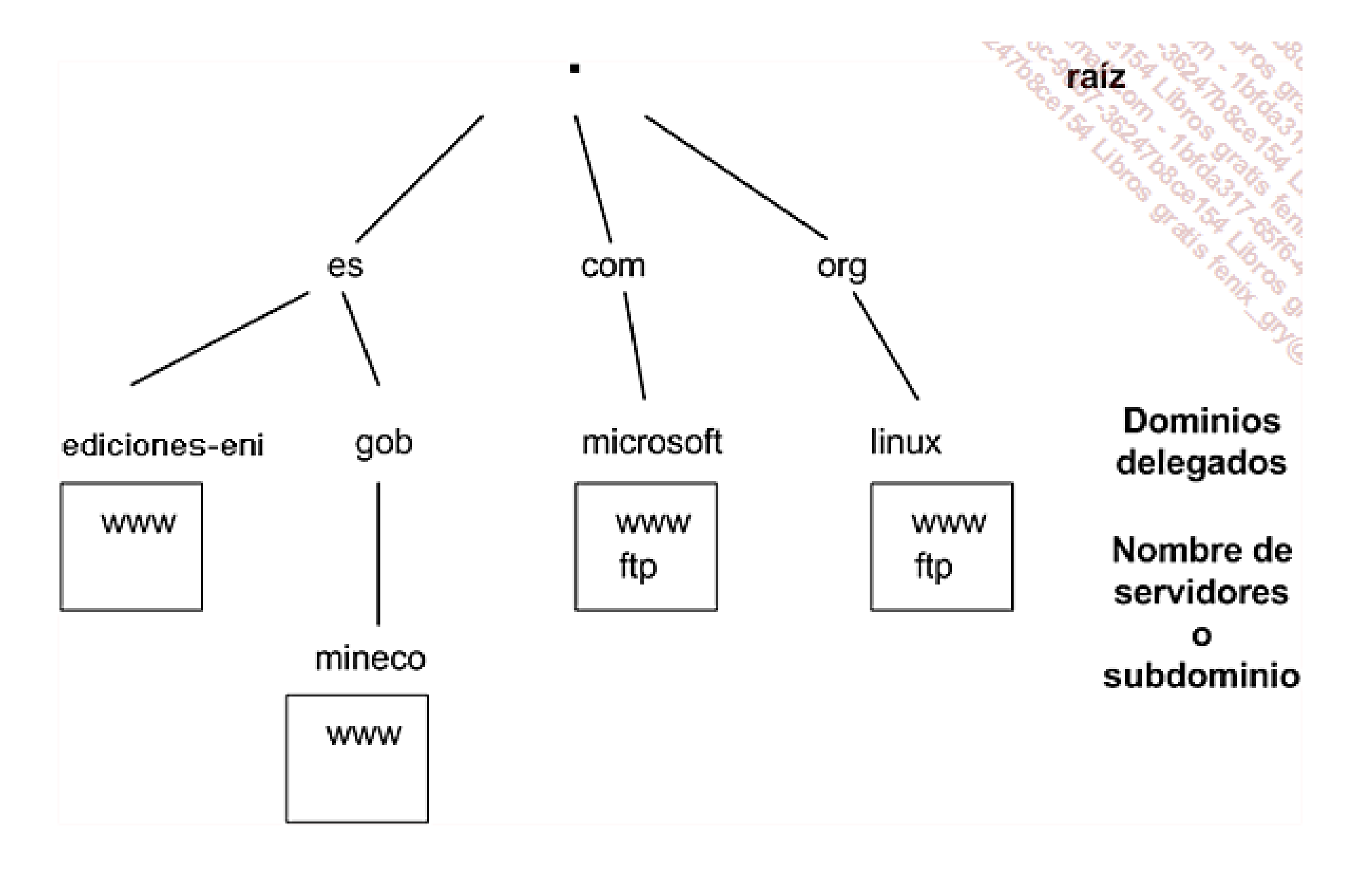
La resolución de dirección en nombre es una funcionalidad que se utiliza como una verificación de identidad y se implementa en UNIX, por ejemplo para verificar el nombre de un servidor del que se tiene que hacer una copia de seguridad cuya dirección IP es conocida o verificar los huéspedes en un entorno NFS (*Network File System*).

El sistema ha evolucionado progresivamente para actuar como un verdadero servicio de localización de recursos: de este modo, hoy en día, un ordenador puede preguntar al servicio DNS para encontrar un servicio de mensajería correspondiente a un dominio específico (registro MX o *Mail eXchanger*), encontrar un servidor Kerberos, un servidor proxy de Internet, un servidor LDAP (*Lightweight Directory Access Protocol*), un servidor SIP (*Session Initiation Protocol*) o incluso localizar un servicio de licencias Microsoft. El SRV Record o registro de servicio permite de este modo definir cualquier tipo de servicio basado en UDP o TCP.

DNS ahora implementa tanto Ipv6 como Ipv4 para identificar los objetos dentro de la arborescencia lógica.

Modelo lógico

El modelo lógico es independiente de la implantación física y permite una implementación completamente distribuida a través de delegaciones y de redirecciones.



Jerarquía de nombres DNS

El detalle de las delegaciones realizadas al nivel del domino raíz y en favor de los dominios de primer nivel (*Top Level Domain* o TLD) está disponible en:http://www.iana.org/domains/root/db/

De este modo, el nombre www.mineco.gob.es corresponde a un alias DNS que resuelve en un dirección IP; en este caso se trata de 193.146.133.11.

```
D:\Windows\system32\cmd.exe - nslookup -
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

D:\Users\Juanki>nslookup -
Servidor predeterminado:  livebox.home
Address:  192.168.1.1

> www.mineco.gob.es
Servidor:  livebox.home
Address:  192.168.1.1

Nombre:  www.mineco.gob.es
Address:  193.146.133.11

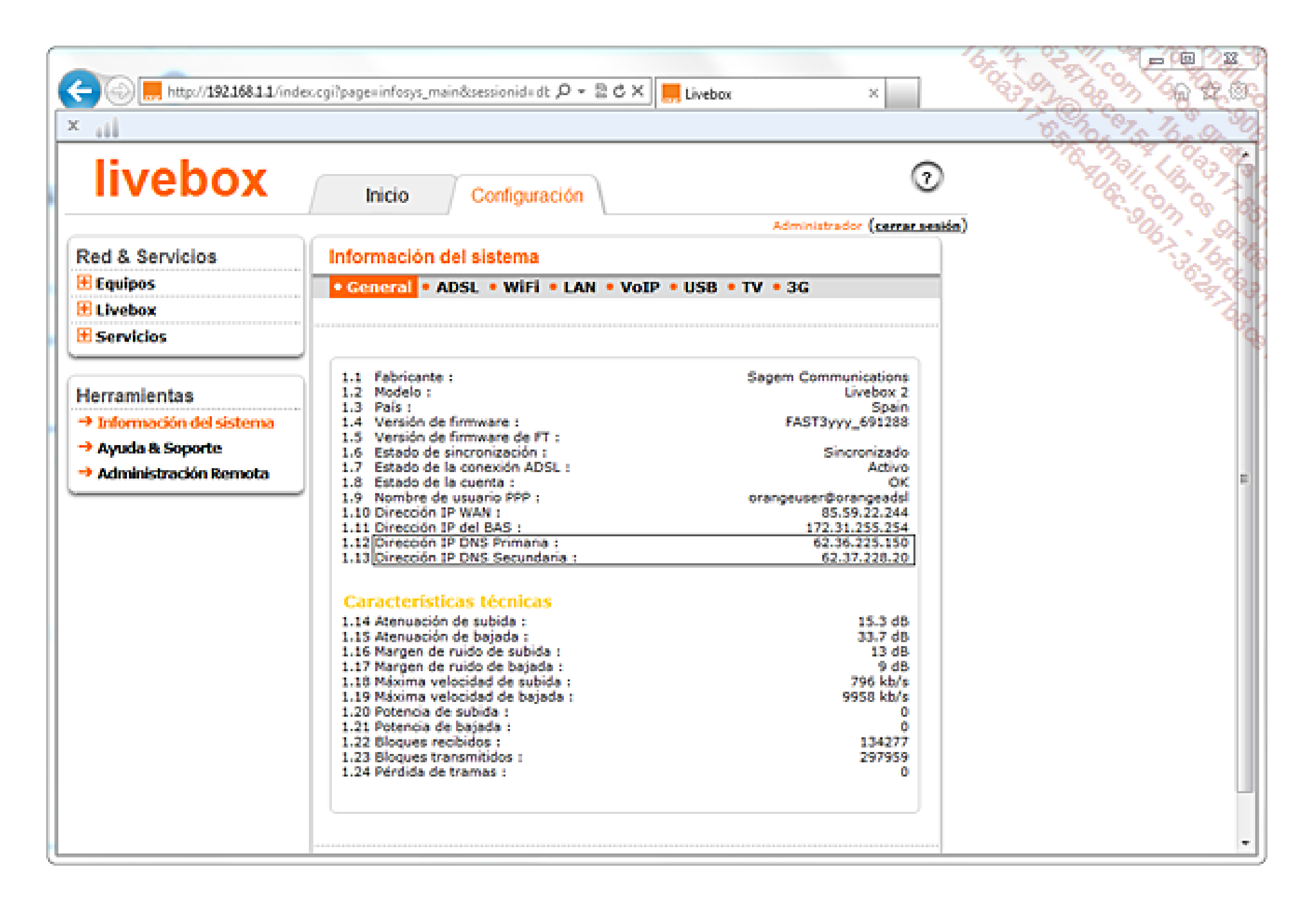
>
```

Un alias DNS es un nombre que reenvía hacia otro nombre. A nivel DNS, se definirá como un CNAME o CANONICAL NAME.

Funcionamiento

Por ejemplo, para un particular, el ordenador obtiene una dirección IP por medio del router ADSL. Entre otras cosas, se le proporciona una dirección IP de DNS. Esta dirección IP es la dirección IP interna del router que va a actuar como proxy DNS (es decir, que va a ser cliente DNS en lugar del

cliente). El router dispone igualmente de una dirección IP externa pública que conoce al menos dos direcciones IP de servidores DNS del proveedor de acceso a Internet (ISP).



Propiedad de la dirección IP pública externa de un router ADSL

De este modo, cuando el ordenador pide resolver un nombre DNS (1), como www.mineco.gob.es, el router ADSL envía esta petición al servidor del ISP (2).

El servidor DNS del ISP pregunta de inmediato a uno de los 13 servidores raíz de Internet (3), para buscar los servidores DNS que gestionan la zona **es**. El servidor raíz, que conoce el servidor que gestiona la zona es, reenvía la dirección IP del servidor DNS correspondiente.

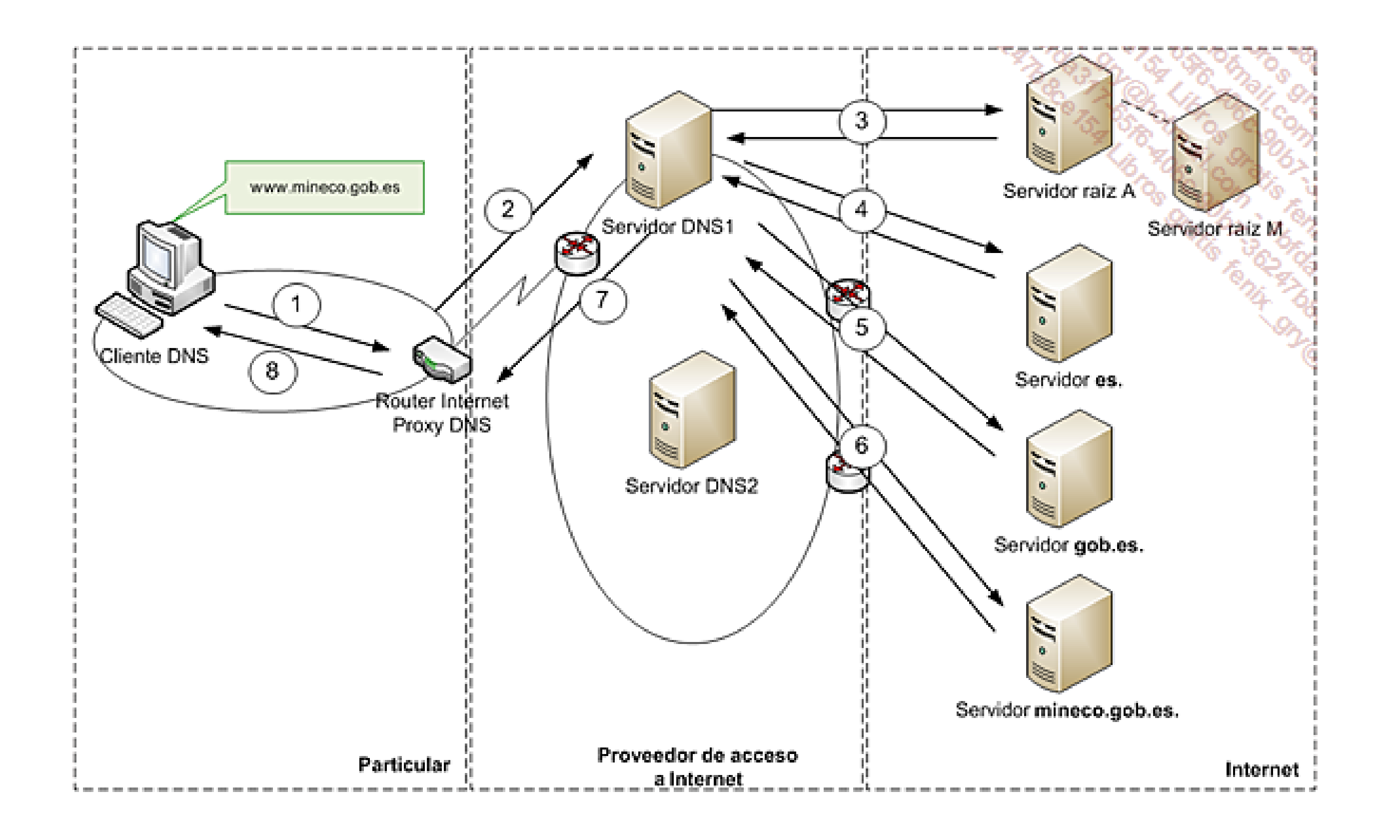
El servidor del ISP a continuación pregunta al servidor que gestiona la zona **fr** (4) para encontrar quién gestiona la zona **gob.es** (5).

Y así, igualmente, hasta que se recupera la dirección IP del servidor DNS que gestiona la zona **mineco.gob.es**.

De hecho, todos los servidores disponen de una caché y puede haber un registro no autorizado (es decir, que no gestiona la zona de destino) que se haya encontrado antes de llegar al servidor autorizado.

Una vez que el servidor DNS del ISP ha obtenido la información que se le ha pedido (en este caso, la dirección IP de www.mineco.gob.es), la pone en la caché, para transmitirla al router ADSL (7).

El router reenvía finalmente la dirección del cliente DNS de la red local (8).



Mecanismo de resolución DNS

Existen dos tipos de peticiones: recursivas e iterativas.

Los intercambios [(1), (8)] y [(2), (7)] corresponden a peticiones recursivas.

Los intercambios (3), (4), (5) y (6) corresponden a peticiones iterativas.

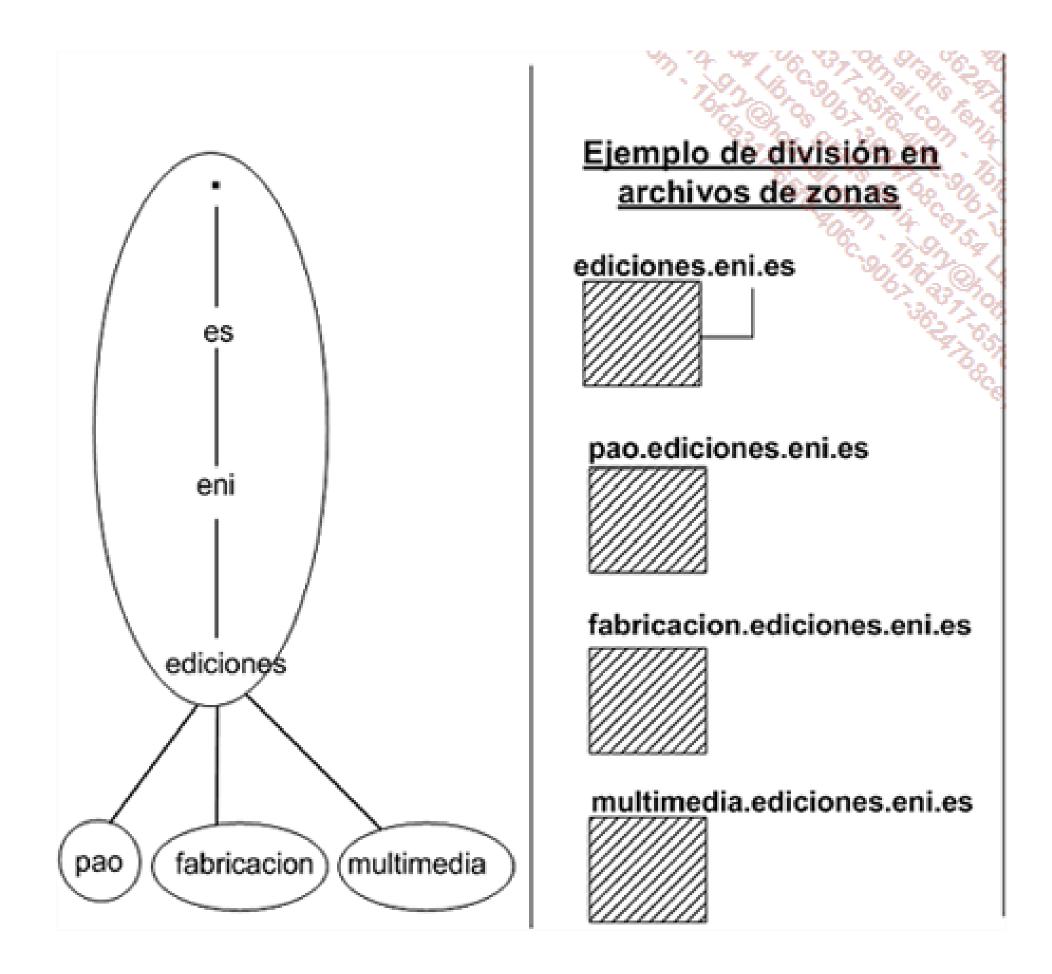
Los servidores raíz que conocen todos los sufijos existentes a nivel mundial están disponibles en la URL: http://www.iana.org/domains/root/servers

Modelo físico

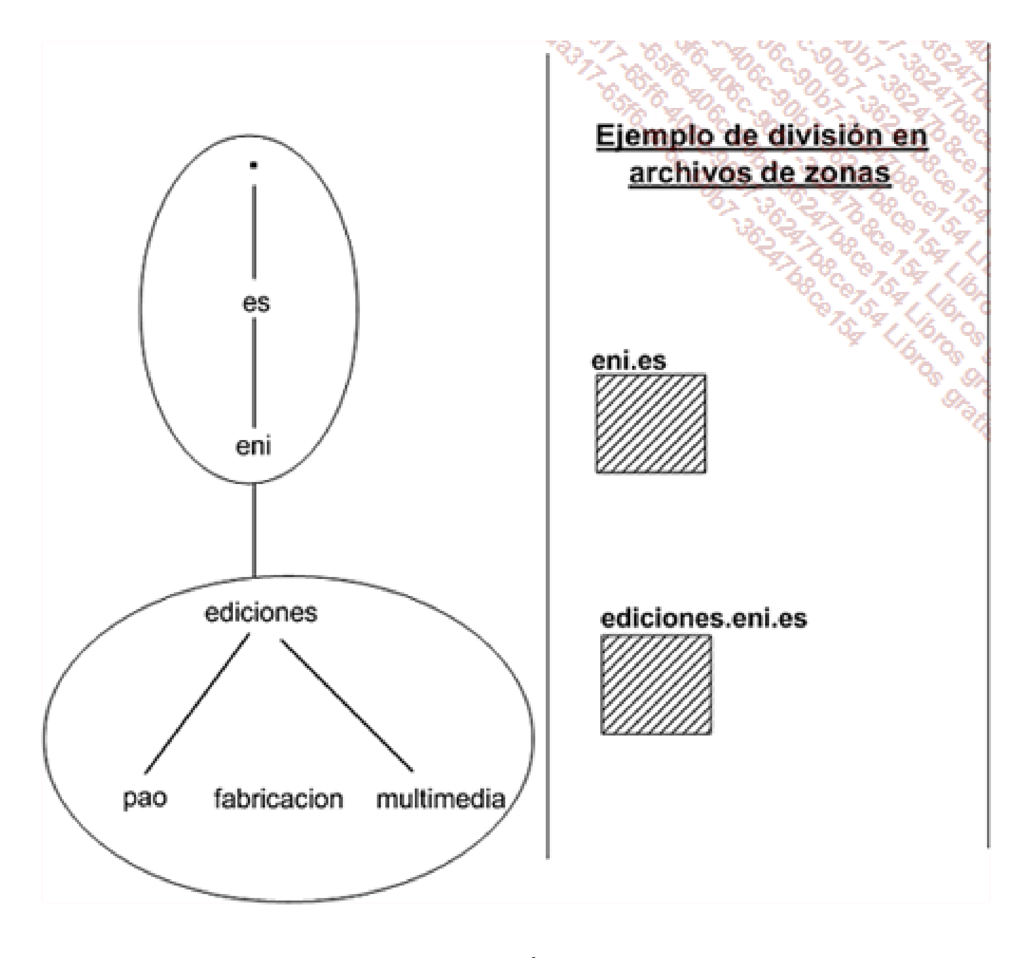
Dadas las arborescencias lógicas DNS, a continuación hay que definir la implementación física de la solución.

Se trata de definir el número de servidores físicos que se utilizarán, el número de zonas o archivos de zonas que se implementarán y la relación entre los diferentes servidores.

Una zona corresponde a un punto de anclaje de una parte de la arborescencia lógica que se materializa mediante un archivo almacenado en un servidor.



Ejemplo 1: división en zonas DNS

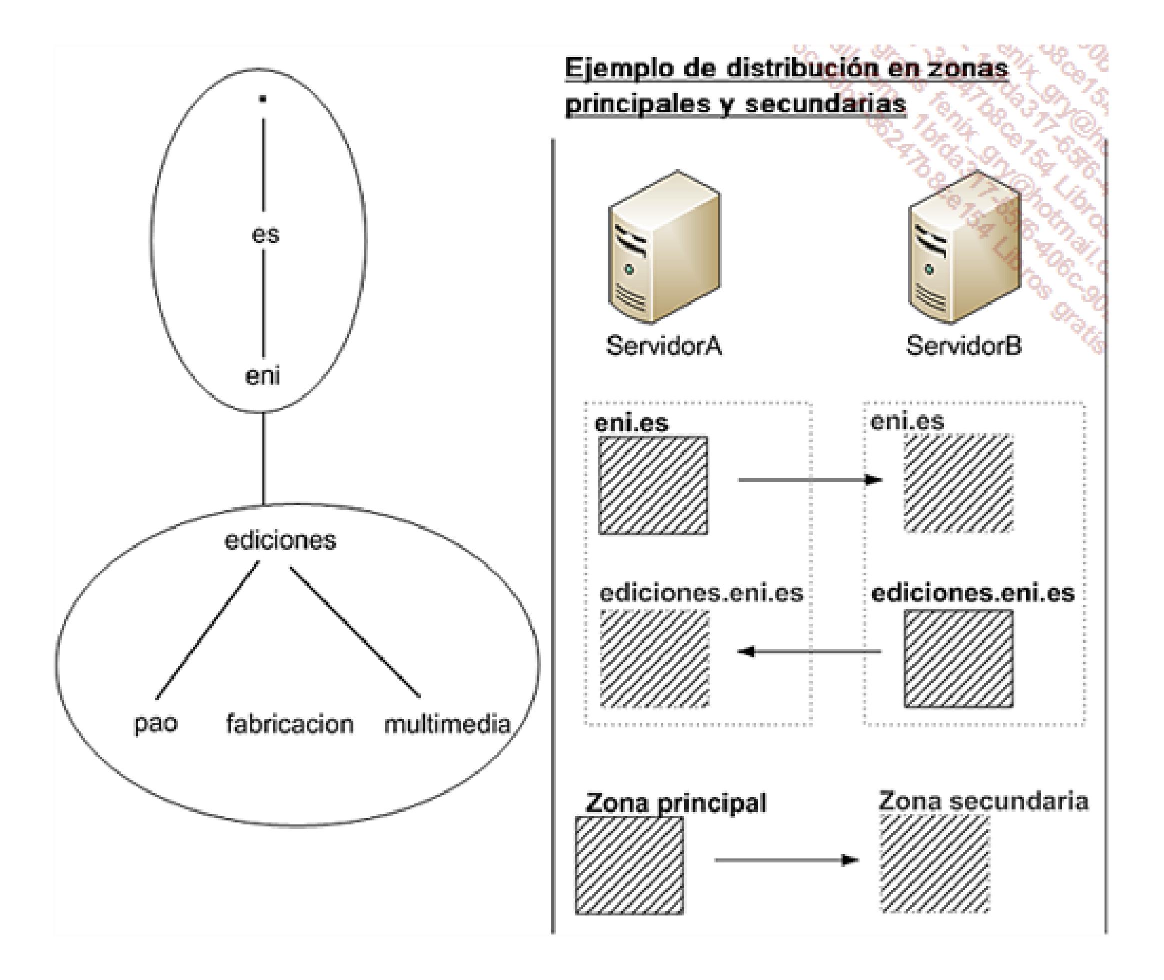


Ejemplo 2: división en zonas DNS

Servidor de nombres

Existen varios tipos de servidores de nombres. El tipo depende del origen a partir del cual el servidor obtiene su información de zona. De este modo, se hablará de **servidor DNS principal**para identificar un servidor que gestiona una zona que se puede modificar. Se calificará como**servidor secundario** aquel que gestiona una zona de solo lectura (copia de una zona principal o secundaria).

Un servidor dispondrá generalmente a la vez de zonas principales y secundarias.



Gestión de zonas principales y secundarias

Por ejemplo, en el esquema anterior, el ServidorA alberga la zona eni.es como zona principal. Se realiza una replicación llamada **transferencia de zona** al ServidorB para esta zona. Inversamente, el ServidorB alberga la zona **ediciones.eni.es** como zona principal. Se hace una copia de esta zona en el ServidorA como zona secundaria.

Generalmente, un servidor alberga también zonas directas, así como varias zonas indirectas (llamadas zonas inversas).

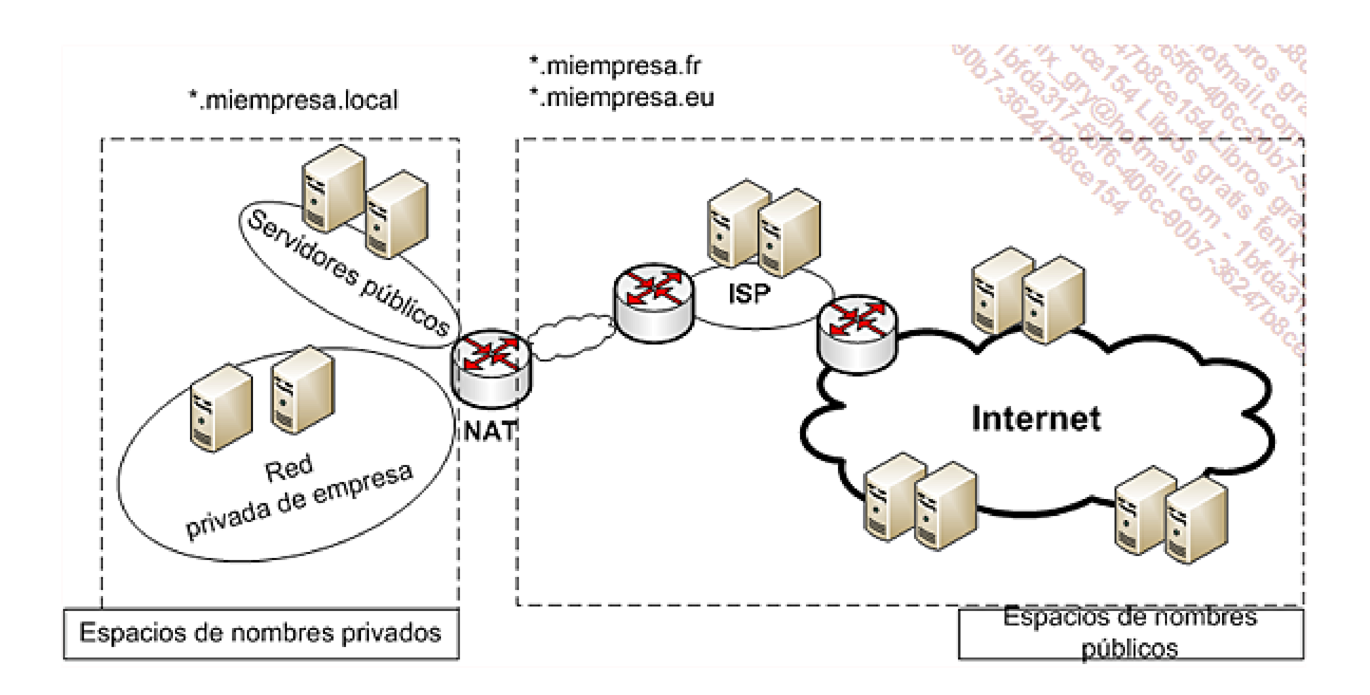
Las zonas inversas son zonas especiales que disponen de un sufijo particular predefinido, **in-addr.arpa**. Estas zonas permiten la resolución de direcciones IP en nombres.

Por ejemplo, para una red privada, se definirán zonas 10.in-addr.arpa, 172.in-addr.arpa y 192.in-addr-arpa.

Espacio de nombres privado y público

Se habla de espacios de nombres para designar los tipos de nomenclatura utilizados. De este modo, dentro de una empresa, los dispositivos y los servidores e incluso los puestos de trabajo recibirán nombres jerárquicos de acuerdo con un espacio de nombres privado. Sería ideal utilizar un sufijo que no exista en internet, por ejemplo ***.local**.

Por el contrario, para referenciar servidores que deben ser accesibles directamente desde Internet, utilizaremos sufijos oficiales, que estén reservados en Internet (por ejemplo *.es, *.eu).



Espacio de nombres públicos y privados

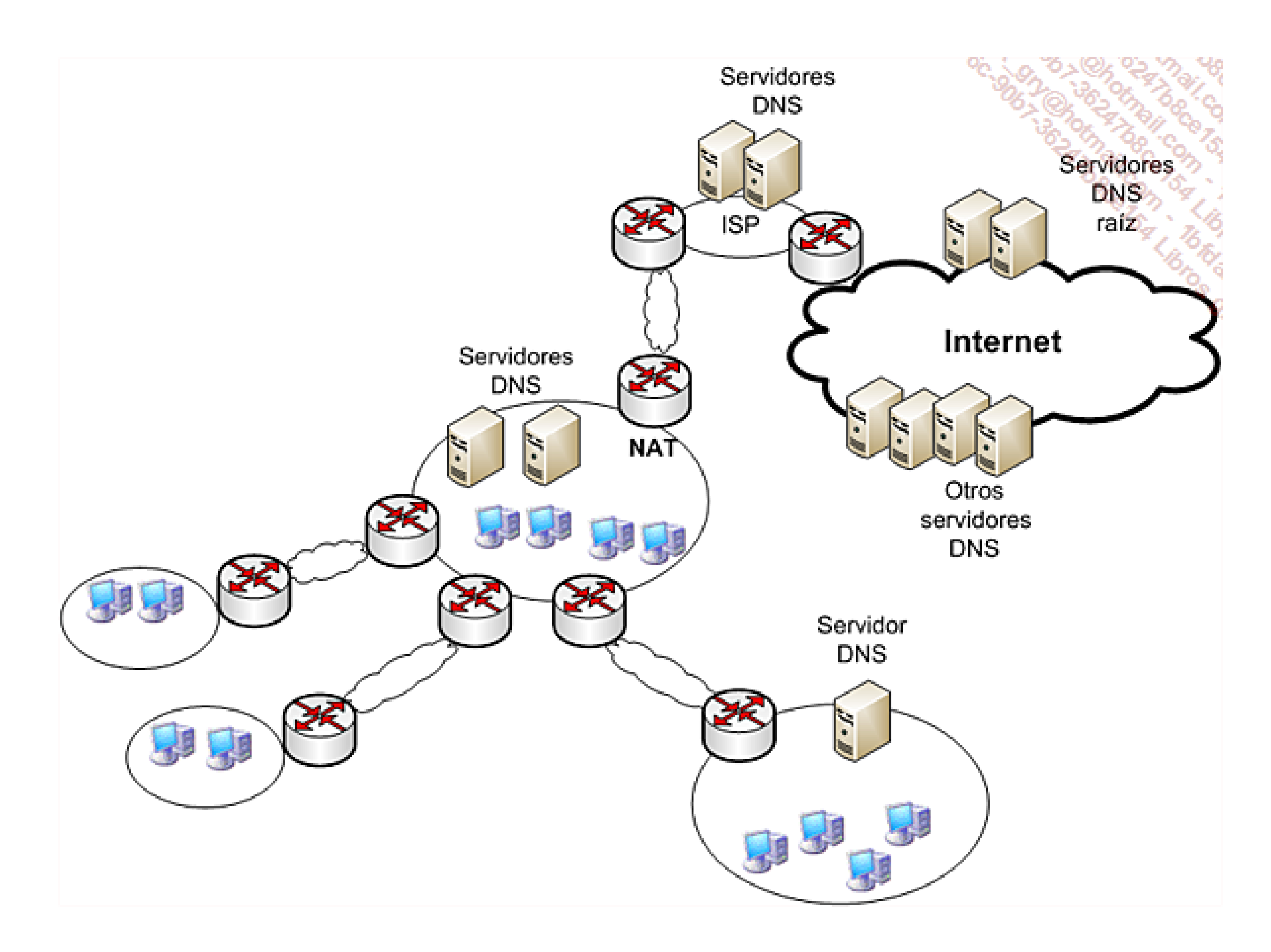
Arquitectura tipo

De manera general, la función de resolución de DNS debe estar disponible **cerca** de los clientes en términos de tiempos de respuesta. Cualquier servidor DNS integra una función de caché centralizada para los clientes. Los clientes disponen de una caché local.

Generalmente, un cliente recibe al menos dos direcciones IP de servidores DNS (para garantizar tolerancia a errores).

Lo ideal es que la configuración DNS se defina en los clientes a través de un servidor DHCP (*Dynamic Host Configuration Protocol*).

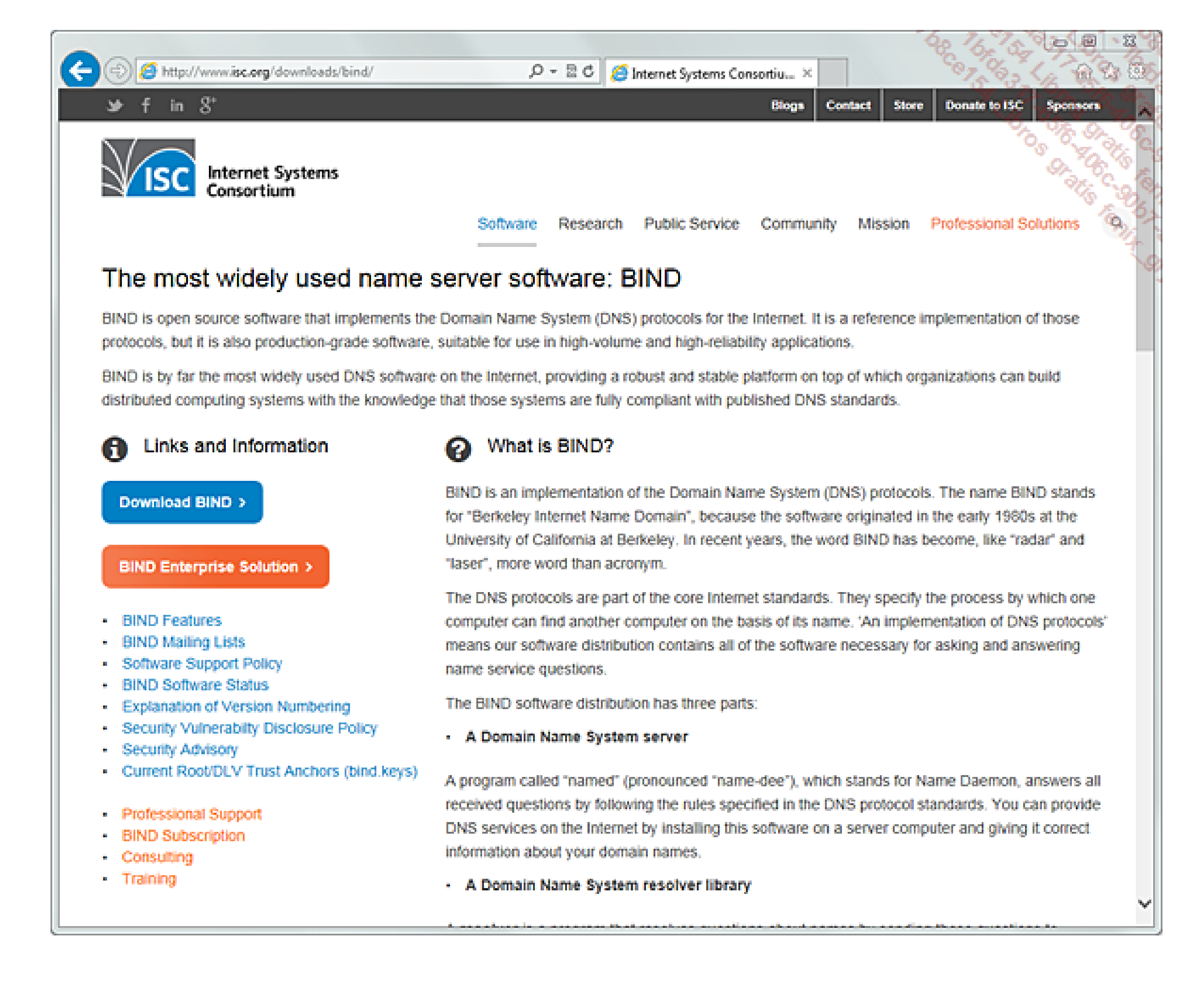
Para los servidores, la configuración DNS se realiza sobre todo manualmente, a menos que en el sistema se hayan hecho reservas DHCP para los servidores.



Arquitectura DNS

Implementaciones

Las principales implementaciones DNS son el software BIND del ISC (*Berkeley Name Domain*del Internet Systems Consortium, al que se puede acceder enhttps://www.isc.org/software/bind) y el servicio DNS de Microsoft proporcionado por los sistemas operativos de servidor.



Página de descarga BIND ISC

b. Dynamic Host Configuration Protocol v.4 (DHCPv4)

Introducción

Históricamente, el servicio DHCP apareció en 1993 como una extensión del protocolo BOOTP creado en 1985. El objetivo de BOOTP es iniciar una estación de trabajo sin disco. La configuración desplegada es personalizable basándose en la dirección MAC de la máquina y asociándole una dirección IP (se habla así de *Reverse Address Resolution Protocol*).

En efecto, el protocolo TCP/IP que se ha impuesto después de muchos años tiene una gran inconveniente: necesita definir para cada uno de los dispositivos como mínimo una dirección IP, una máscara, así como ocasionales parámetros complementarios.

El servicio DHCP permite definir de manera centralizada una configuración TCP/IP completa para el conjunto de los dispositivos de red (parámetros dinámicos o estáticos).

Diferentes RFC definen BOOTP y DHCP:

- RFC 951: BOOTP
- RFC 1497: opciones BOOTP vendor extensions
- RFC 1541: definición del protocolo DHCP
- RFC 1542: interacción entre BOOTP y DHCP
- RFC 2131: DHCP
- RFC 2132: complemento a las opciones DHCP y BOOTP vendor extensions

 Puede consultar estas RFC en http://www.ietf.org/rfc/

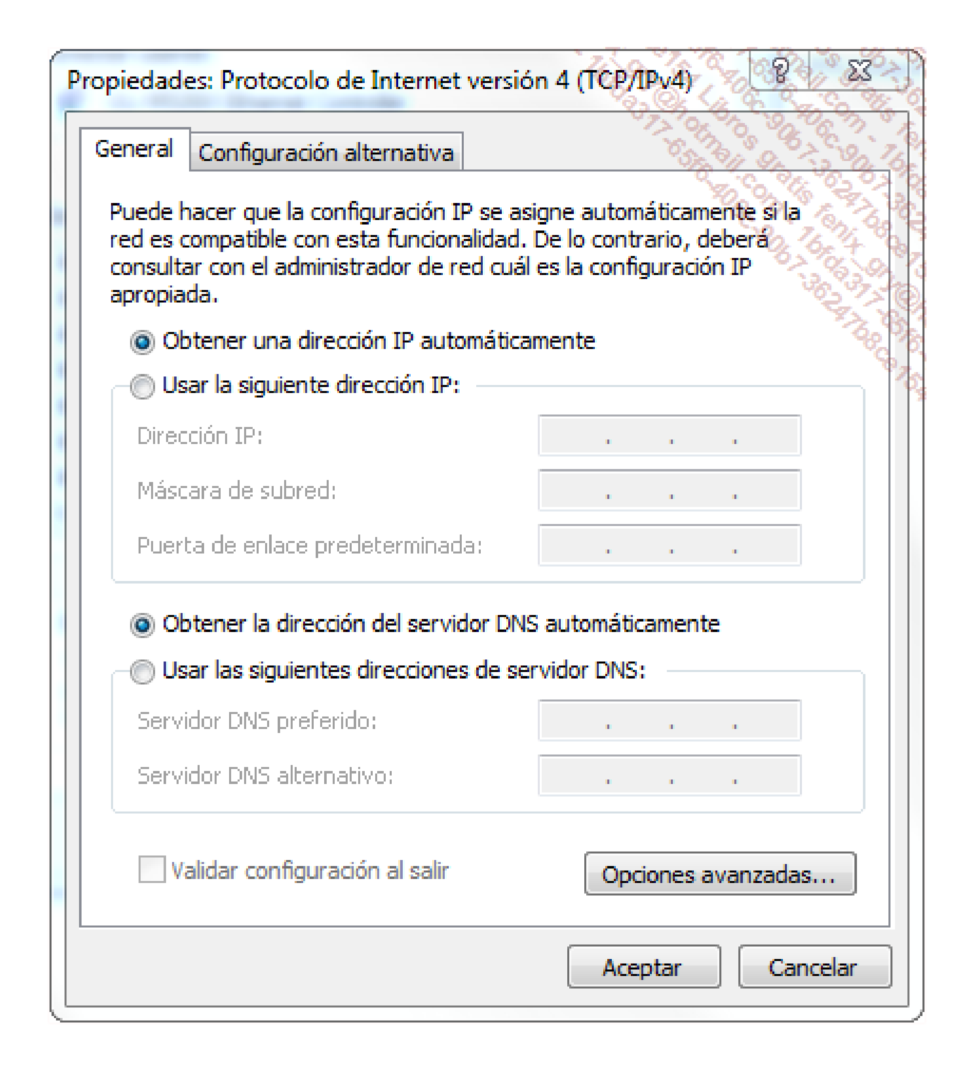
Funcionamiento en una pequeña red

Un dispositivo, un puesto de trabajo, un teléfono IP, un lector de código de barras Wi-Fi, una impresora de red, etc., ejecutan un componente cliente DHCP que les permite comunicarse con un servidor para obtener un conjunto de parámetros TCP/IP.

Se utiliza cada vez más a menudo una reserva de dirección IP asociada a una dirección MAC. Este mecanismo permite disponer de IP fijas conservando flexibilidad de gestión al definir los ordenadores como clientes DHCP.

En general, el dispositivo se configura por defecto para utilizar un servidor DHCP.

Por ejemplo, en Windows 7:



Configuración DHCP en Windows 7

O en Linux:

```
root@CentOs:~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

              Configuración de Red

  Nombre                                    eth0
  Dispositivo                               eth0
  Usar DHCP                                 [*]
  IP Estática
  Máscara de red
  IP de la puerta de enlace predeterminada
  Servidor de DNS Primario
  Servidor de DNS Secundario

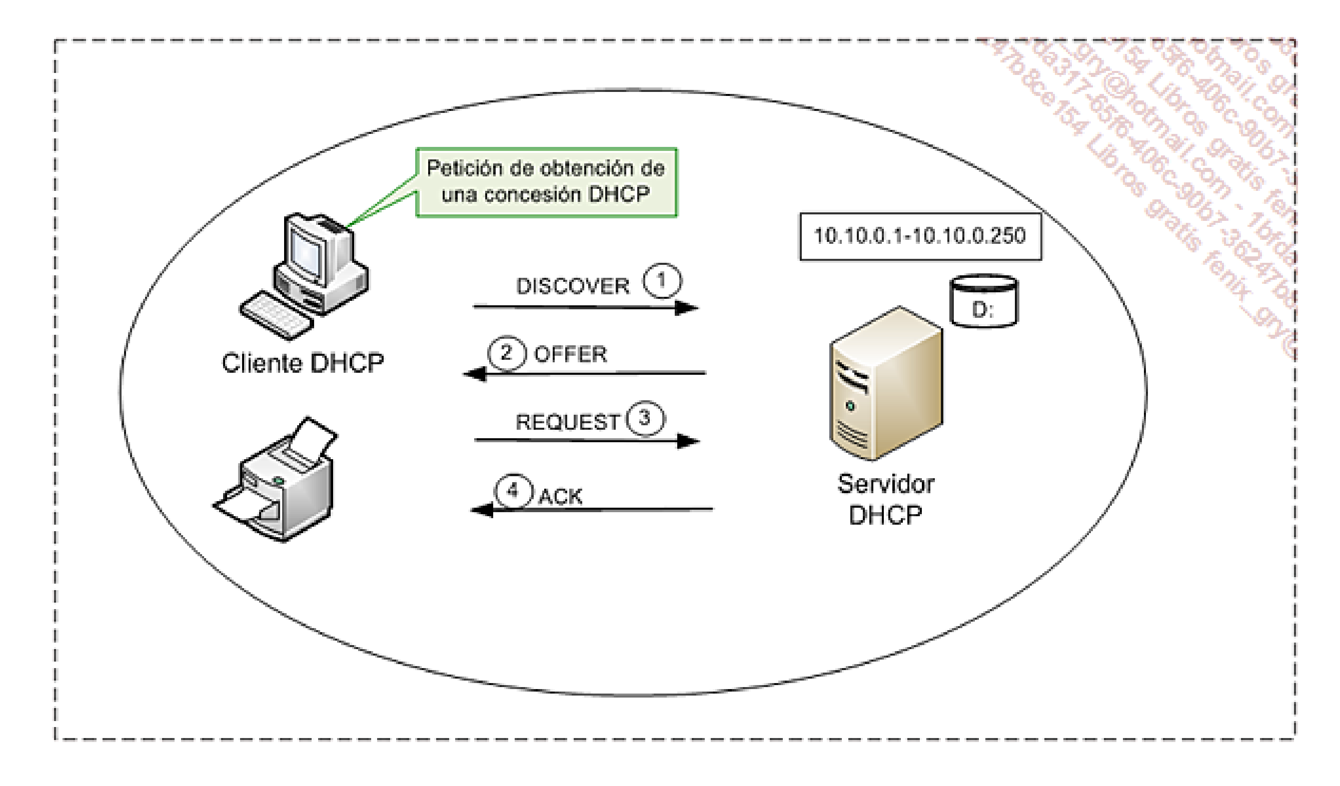
          Aceptar                  Cancelar

<Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

Configuración DHCP en CentOS 6.3

Al arrancar la primera vez, la comunicación que permite obtener la configuración se desarrolla en varias etapas:

- (1) DHCP DISCOVER: el descubrimiento de la red.
- (2) DHCP OFFER: la propuesta de parámetros por parte de uno o varios servidores.
- (3) DHCP REQUEST: la respuesta favorable del cliente a una de las propuestas.
- (4) DHCP ACK: el acuse de recibo por el servidor teniendo en cuenta la petición del cliente.



DHCP DISCOVER

El protocolo TCP/IP se inicializa con una versión limitada (dirección IP no definida: 0.0.0.0).

Transmite en el nivel 2 a todos los ordenadores (FF.FF.FF.FF.FF.FF) una petición para obtener una concesión DHCP. Como se trata de un protocolo UDP, la dirección IP debe ser emitida por el destino. Se define como 255.255.255.255 (todo el mundo).

```
▷ Frame 297: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
▷ Ethernet II, Src: a0:88:b4:d9:4c:7c (a0:88:b4:d9:4c:7c), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
▷ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
▷ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
▽ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x9c4c1195
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: a0:88:b4:d9:4c:7c (a0:88:b4:d9:4c:7c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▷ Option: (53) DHCP Message Type
  ▷ Option: (61) Client identifier
  ▷ Option: (50) Requested IP Address
  ▷ Option: (12) Host Name
  ▷ Option: (60) Vendor class identifier
  ▷ Option: (55) Parameter Request List
  ▷ Option: (255) End
```

Análisis de una trama DHCP DISCOVER

Capa	Origen (cliente)	Destino (todo el mundo)
UDP	68	67
IP	0.0.0.0	255.255.255.255
Ethernet	a0:88:b4:d9:4c:7c	ff:ff:ff:ff:ff:ff

Si al cabo de un segundo el cliente no ha recibido ninguna respuesta, se transmite una nueva petición al cabo de 9, 13 y 16 segundos.

Después de estos intentos, se hará una petición cada cinco minutos.

DHCP OFFER

Algunos dispositivos que actúan como servidor DHCP (servidor, router, router ADSL) responden al cliente.

Transmiten una propuesta que tiene la siguiente información: la dirección MAC del cliente, una dirección IP, una máscara de subred, la duración de la concesión y su dirección IP.

Capa	Origen (servidor)	Destino (cliente)
UDP	67	68
IP	192.168.1.1	192.168.1.92
Ethernet	00:25:15:21:f1:20	a0:88:b4:d9:4c:7c

```
▷ Frame 298: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
▷ Ethernet II, Src: 00:25:15:21:f1:20 (00:25:15:21:f1:20), Dst: a0:88:b4:d9:4c:7c (a0:88:b4:d9:4c:7c)
▷ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.92 (192.168.1.92)
▷ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
▽ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x9c4c1195
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.1.92 (192.168.1.92)
    Next server IP address: 192.168.1.1 (192.168.1.1)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: a0:88:b4:d9:4c:7c (a0:88:b4:d9:4c:7c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▷ Option: (53) DHCP Message Type
  ▷ Option: (54) DHCP Server Identifier
  ▷ Option: (51) IP Address Lease Time
  ▷ Option: (58) Renewal Time Value
  ▷ Option: (59) Rebinding Time Value
  ▷ Option: (28) Broadcast Address
  ▷ Option: (3) Router
  ▷ Option: (6) Domain Name Server
  ▷ Option: (1) Subnet Mask
  ▷ Option: (255) End
    Padding
```

Análisis de una trama DHCP OFFER

El cliente selecciona una propuesta (en general, la primera que recibe).

Tenga en cuenta que, después de la RFC, el servidor intenta primero un *unicast* (para encargarse de una eventual transmisión DHCP) antes de hacer una difusión.

DHCP REQUEST

Esta respuesta permite al cliente avisar a todos los servidores que se ha captado una concesión. La información relativa a la concesión está disponible al final de la trama.

Así, el resto de los servidores pueden retirar su propuesta y dejar disponible la dirección que se había reservado.

Capa	Origen (cliente)	Destino (todo el mundo)
UDP	68	67
IP	0.0.0.0	255.255.255.255
Ethernet	a0:88:b4:d9:4c:7c	ff:ff:ff:ff:ff:ff

```
▷ Frame 299: 393 bytes on wire (3144 bits), 393 bytes captured (3144 bits) on interface 0
▷ Ethernet II, Src: a0:88:b4:d9:4c:7c (a0:88:b4:d9:4c:7c), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
▷ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
▷ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
▽ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x9c4c1195
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: a0:88:b4:d9:4c:7c (a0:88:b4:d9:4c:7c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▷ Option: (53) DHCP Message Type
  ▷ Option: (61) Client identifier
  ▷ Option: (50) Requested IP Address
  ▷ Option: (54) DHCP Server Identifier
  ▷ Option: (12) Host Name
  ▷ Option: (81) Client Fully Qualified Domain Name
  ▷ Option: (60) Vendor class identifier
  ▷ Option: (55) Parameter Request List
  ▷ Option: (255) End
```

Análisis de una trama DHCP REQUEST

DHCP ACK

El servidor cuya propuesta ha sido aceptada envía una trama dirigida directamente al cliente como acuse de recibo. Se añaden otras opciones a la trama (opción 003 router, 006 Domain Name Server, 001 Subnet Mask).

Capa	Origen (servidor)	Destino (cliente)
UDP	67	68
IP	192.168.1.1	192.168.1.92
Ethernet	00:25:15:21:f1:20	a0:88:b4:d9:4c:7c

```
▷ Frame 300: 354 bytes on wire (2832 bits), 354 bytes captured (2832 bits) on interface 0
▷ Ethernet II, Src: 00:25:15:21:f1:20 (00:25:15:21:f1:20), Dst: a0:88:b4:d9:4c:7c (a0:88:b4:d9:4c:7c)
▷ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.92 (192.168.1.92)
▷ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
▽ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x9c4c1195
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.1.92 (192.168.1.92)
    Next server IP address: 192.168.1.1 (192.168.1.1)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: a0:88:b4:d9:4c:7c (a0:88:b4:d9:4c:7c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▷ Option: (53) DHCP Message Type
  ▷ Option: (54) DHCP Server Identifier
  ▷ Option: (51) IP Address Lease Time
  ▷ Option: (58) Renewal Time Value
  ▷ Option: (59) Rebinding Time Value
  ▷ Option: (28) Broadcast Address
  ▷ Option: (81) Client Fully Qualified Domain Name
  ▷ Option: (3) Router
  ▷ Option: (6) Domain Name Server
  ▷ Option: (1) Subnet Mask
  ▷ Option: (255) End
```

Análisis de una trama DHCP ACK

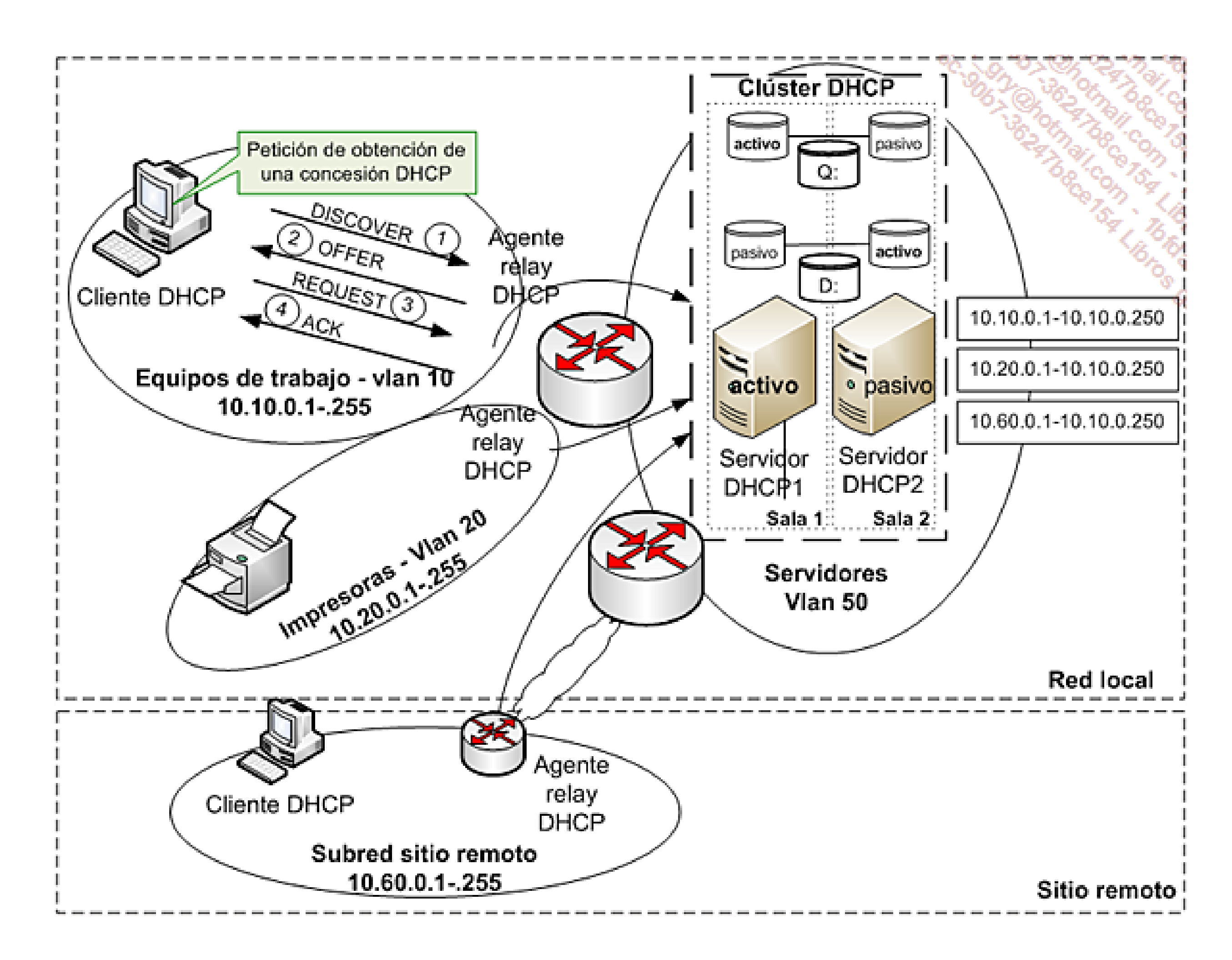
Tenga en cuenta que, en algunas implementaciones de DHCP, el ACK se puede realizar con una difusión.

Funcionamiento en una gran red

En un entorno más grande, la arquitectura es un poco más compleja. Por una parte, las subredes IP están generalmente asociadas a una descomposición en VLAN. Así, se va a asignar una VLAN por tipo de dispositivos (estación de trabajo, servidor, lector de códigos de barras) o por uso (red principal, copias de seguridad, administración de servidores).

Por otra parte, como los clientes están generalmente en subredes diferentes que los servidores DHCP, conviene implementar un mecanismo que permita transmitir las tramas DHCP a o desde los servidores DHCP designados. De hecho, los routers detienen las tramas de difusión.

El comando asociado generalmente a los routers es «ip-helper-address». Permite designar explícitamente uno o varios servidores DHCP hacia el que se transmitirá una difusión DHCP captada en la red local.



Funcionamiento DHCP en un entorno enrutado

En un entorno consecuente, el núcleo de la red está constituido generalmente por un conmutador multinivel que conoce todas las VLAN. Cada una de las interfases que corresponden a la puerta de enlace por defecto conoce la existencia del servidor al que va a redirigir las difusiones DHCP.

Clúster DHCP

El servidor DHCP se podrá ayudar de un clúster que va a ofrecer redundancia del servicio, al mismo tiempo que redundancia de los datos:

- Un disco D: contiene la configuración del servidor DHCP cuyo servicio se ejecuta en uno de los dos servidores. El servicio DHCP del otro servidor está en *standby*.
- Un disco Q corresponde al quórum. Almacena la información de actual del clúster. En caso de problemas, el servidor que puede acceder al quórum se hace cargo.

Los recursos de disco se replican en segundo plano en modo síncrono, para permitir una recuperación en caso de fallo de un disco o de la pérdida de una sala.

La dirección IP que referencia el servicio DHCP es de hecho una dirección IP virtual, que corresponde a un recurso del clúster. Este recurso se ejecuta efectivamente en uno de los nodos del clúster.

DHCP Failover

Esta funcionalidad permite asegurar la continuidad del servicio DHCP sin necesitar un clúster para bascular. De hecho, Windows Server 2012 o ISC DHCP ofrece esta funcionalidad. De este modo, los servidores son capaces de intercambiar su información.

Agente relay DHCP

La utilización de agentes relay introduce un funcionamiento complementario.

Cuando la puerta de enlace recibe una trama DHCP que proviene de un cliente de su subred, el router transmite la trama dirigida directamente al servidor DHCP. Si la dirección IP origen identificada es 0.0.0.0, el router la sustituye por su propia dirección IP de puerta de enlace. De hecho, el servidor DHCP debe poder identificar el área de alcance DHCP para asignar una dirección IP válida al cliente.

El servidor DHCP recibe entonces la petición y examina la dirección IP de origen para asociar un rango de dirección IP adecuado.

Selecciona finalmente una dirección IP disponible para enviar una propuesta directamente a la puerta de enlace. La puerta de enlace finalmente va a transmitir la propuesta a la subred local (al destino del puesto de trabajo que hace la petición en el nivel 2 y de todo el mundo en el nivel 3).

A continuación, el router transmite el mensaje DHCP REQUEST al servidor DHCP.

Finalmente, el servidor responde un DHCP ACK al cliente.

Renovación de la concesión

El cliente obtiene los parámetros TPC/IP para una duración limitada: la concesión.

Esta concesión se debe renovar regularmente para permitir al cliente seguir utilizando sus parámetros.

La renovación se produce después de que expire la mitad de la concesión. Si la petición no obtiene resultados, se realiza un nuevo intento a 7/8 de la duración de la concesión.

 Este mecanismo de renovación evita generar tráfico de difusión inútil.

Cuando un equipo arranca, se repite el proceso completo; esto permite tener en cuenta los desplazamientos de los ordenadores portátiles.

El servidor también puede pedir al cliente que libere su dirección dirigiéndole un DHCP NACK.

Arquitectura tipo

Una arquitectura tipo implementa generalmente un servidor centralizado para el conjunto de la red. Por lo común, para tener en cuenta las posibles interrupciones de conexiones remotas, se configuran las concesiones para una duración lo suficientemente larga.

Igualmente es posible centralizar de forma completa la gest

Comprensión de la necesidad de la seguridad

Conocer los fallos potenciales y las necesidades de protección de su red es un tema importante. Esta toma de conciencia es reciente. Por ejemplo, muchos de los protocolos que se utilizan no se diseñaron originalmente para ser protocolos seguros. Entre ellos, la mayoría de los relacionados con TCP/IP.

Las interconexiones entre los sistemas se multiplicaron, especialmente a través de la red pública Internet, donde aparecieron numerosos fallos. No se puede pensar en eliminar absolutamente todos los riesgos, pero se pueden reducir conociéndolos y adoptando las medidas adecuadas.

1. Garantías exigidas

La seguridad en red se basa en cuatro puntos clave:

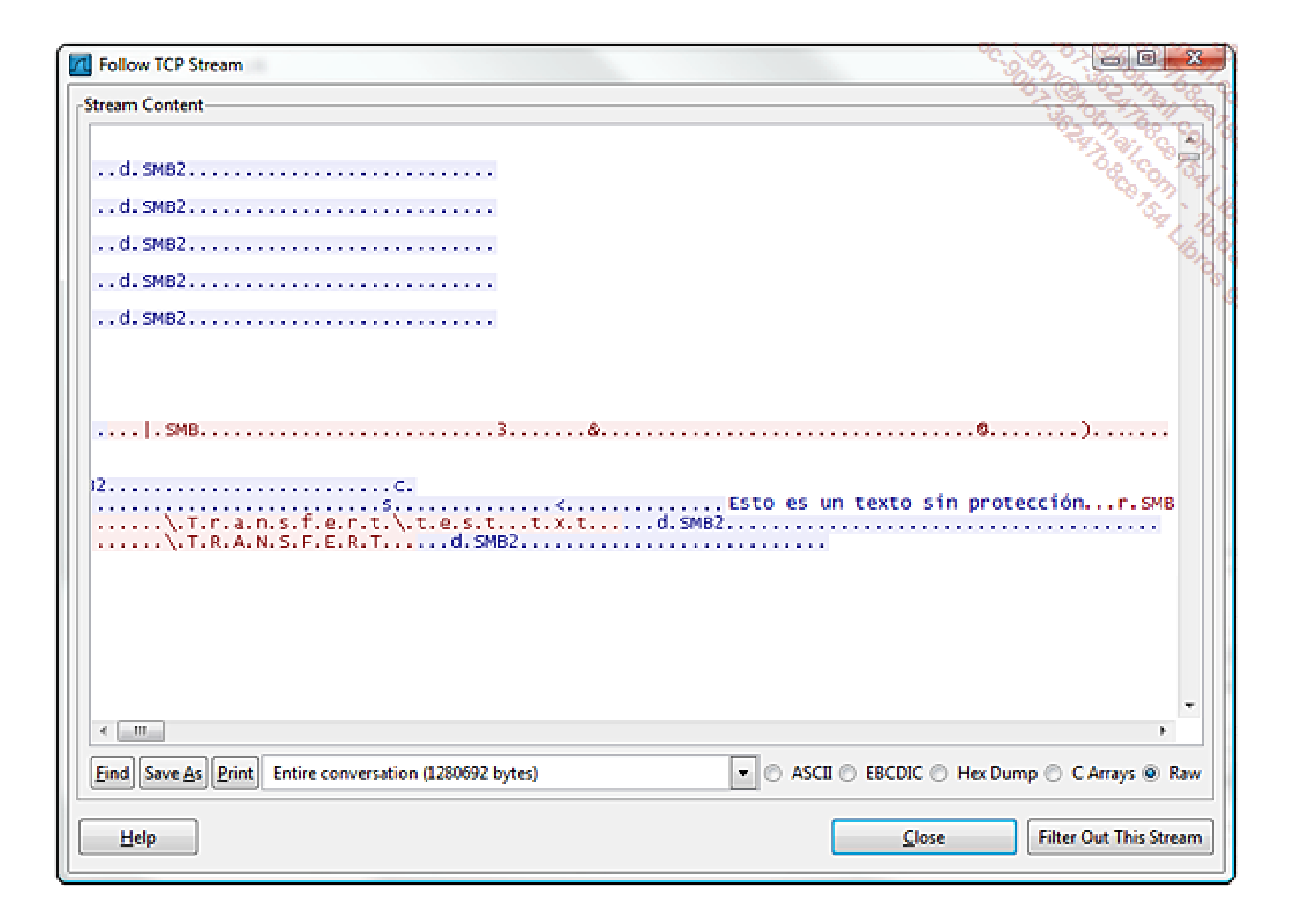
- La autentificación, que permite asegurar la identidad para conocer el origen de las comunicaciones.
- La confidencialidad, que tiene por objetivo evitar cualquier fuga de información.
- La integridad, para prohibir o conocer las modificaciones y evitar pérdidas de información.
- La disponibilidad, que permite asegurar un servicio en todo momento.

Como complemento a estos cuatros temas, se puede mencionar el concepto de la no-denegación, cuyo objetivo es garantizar, en cualquier circunstancia, el origen de una comunicación o de una transferencia de datos. Para ello, recupera un concepto familiar de nuestra vida cotidiana, como es la firma, pero en formato electrónico.

2. Peligros latentes

a. La circulación de los datos

En muchas redes, la parte fundamental, o más bien la totalidad de las comunicaciones, transitan sin protección. El contenido es legible por cualquiera.



Extracto de la reconstrucción de una trama de red

El análisis de tramas anterior corresponde a una solicitud de apertura de un archivo almacenado en un servidor, hecha desde un equipo de trabajo. Podemos ver que su contenido, «esto es un texto sin protección», se ha reconstruido a través de la comunicación de red.

b. Protocolos de Red y Transporte

Los protocolos de comunicación de red pueden ser el objetivo de ataques dirigidos a sus componentes, es decir, a sus cabeceras.

Se conocen numerosos métodos para esto. Se han utilizado ampliamente las diferentes capas de un modelo como TCP/IP, en que los dos niveles, Red y Transporte, tienen algunas inconsistencias.

Por ejemplo, en *Internet Protocol* (IP), se puede suplantar la asignación lógica de direcciones. Igualmente se pueden manipular las operaciones de fragmentación/defragmentación.

Internet Control Message Protocol (ICMP), y el uso de los comandos «ping», fue objeto de numerosos ataques.

Se puede aprovechar el establecimiento de conexión (3-way handshake) del protocolo *Transmission Control Protocol* (TCP) para apropiarse de las comunicaciones.

Esto no son más que algunas operaciones, pero existen muchas más. Afortunadamente, la experiencia ha permitido convertir estos protocolos en más fiables. De hecho, el software que los controla tiene en cuenta desde hace algún tiempo los antecedentes de los numerosos ataques que se han intentado.

Aunque no estén al abrigo de nuevas tentativas, los riesgos se reducen cada vez más.

c. Protocolos aplicativos estándares

Las últimas amenazas contemplan sobre todo las capas altas. Protocolos aplicativos estándares

de TCP/IP, como *HyperText Transfer Protocol* (HTTP), *Simple Mail Transfer Protocol*(SMTP), *File Transfer Protocol* (FTP), *Domain Name System* (DNS), están especialmente amenazados. De hecho, se utilizan con tanta frecuencia que encontrar fallos de seguridad es muy sencillo.

Estos protocolos aplicativos, como los de nivel inferior, presentan numerosos fallos de seguridad debido a que su diseño es antiguo. Incluso podemos decir que es la interpretación del software la que conlleva los principales problemas.

Por ejemplo, la utilización de páginas dinámicas en Internet, cada vez más avanzada, y la de los programas complementarios, implica una programación cada vez más compleja de los navegadores Web. Constantemente se descubren nuevos fallos que se deben corregir.

El uso de archivos adjuntos en el correo electrónico permitió una nueva posibilidad de propagación de los virus.

d. Protocolos de capas bajas

En el nivel más bajo, la protección no debe dejarse de lado, cualquiera que sea el tamaño de la red. A nivel local, el uso de conmutadores, para la interconexión de ordenadores a Ethernet, implica la protección de este protocolo. También se debe implantar seguridad para Wi-Fi.

Si la comunicación sobrepasa el ámbito de la empresa, debe ser una prioridad atenuar los peligros potenciales.

e. Riesgos a nivel de software

Los equipos en la red se han vuelto complejos. Los conmutadores, como los routers, proporcionan funciones muy importantes. Son controlados por verdaderos sistemas operativos que, como cualquier aplicación informática de red, contiene fallos potencialmente aprovechables para un ataque.

Es necesario proteger los medios de administración y las cuentas asociadas.

Estos sistemas operativos se deben actualizar igual que los servidores y los equipos de trabajo.

Herramientas y tipos de ataques

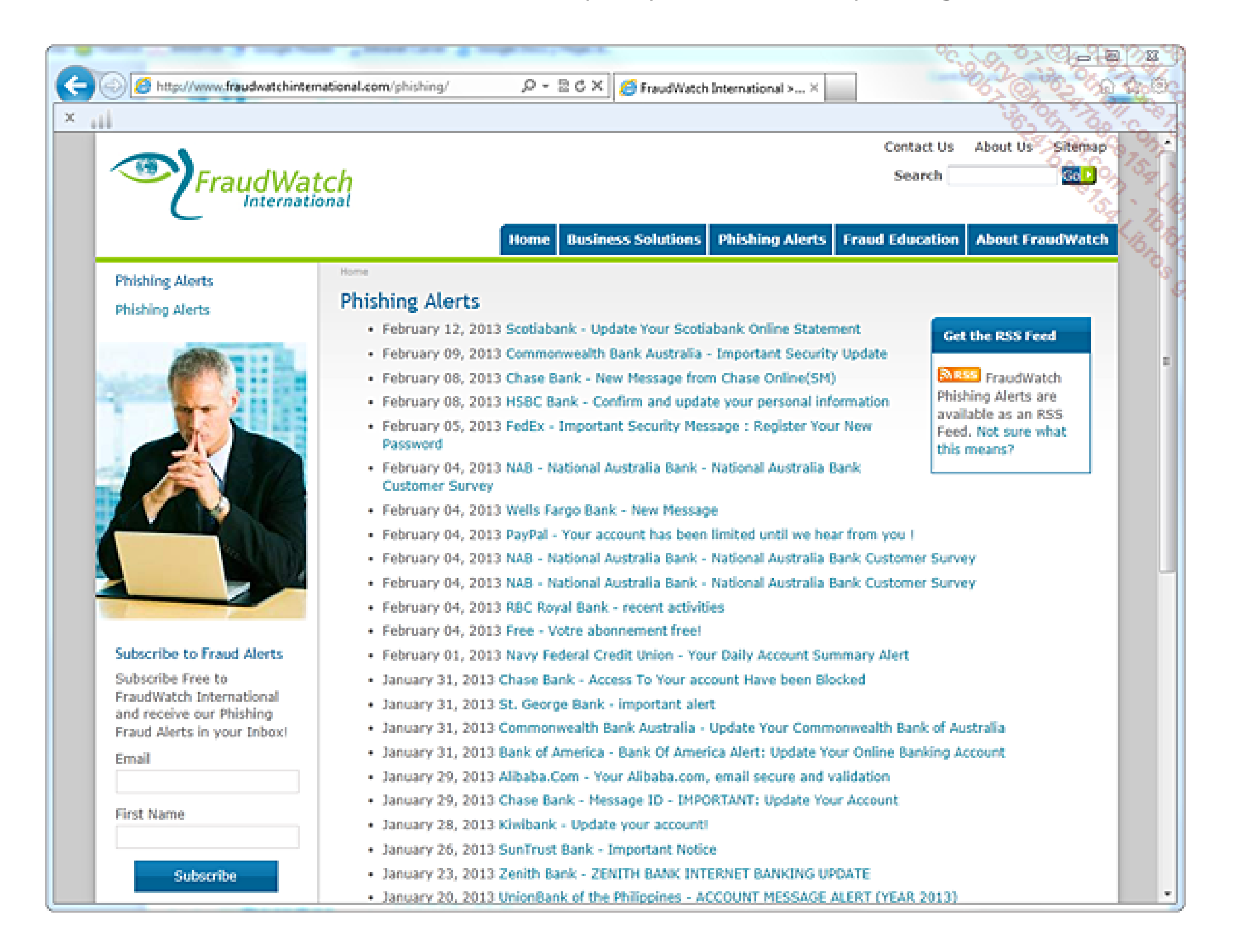
Además de la penetración en un sistema, los ataques por denegación del servicio (DoS - *Denial of Service*) son muy frecuentes. Tienen como objetivo solicitar un servicio de red repetidamente hasta que este no puede responder a las solicitudes legítimas, e incluso se para. Para conseguir una mayor eficacia, puede ser que miles de máquinas ataquen simultáneamente. Se habla de denegación de servicio distribuida (DDoS - *Distributed Denial of Service*).

1. Ingeniería social

Esta técnica, llamada en inglés «social engineering», consiste en manipular a las personas para eludir los dispositivos de seguridad. Considerando que el ser humano es el eslabón débil en un Sistema de Información, se utilizan la ignorancia o la credulidad del usuario común.

La estafa mediante el *phishing*, compuesta por las palabras inglesas *phreaking*, (piratería de líneas telefónicas) y *fishing* (pesca), es una variante muy eficaz. Este timo consiste en un envío por correo electrónico para incitar al usuario a divulgar sus datos confidenciales, como por ejemplo los bancarios. Primero se envía un correo electrónico que contiene un enlace a un sitio web falso que imita a uno real. A menudo el objetivo es obtener el número de la tarjeta de crédito.

El sitio fraudwatchinternational.com resume las principales alertas de phishing existentes:

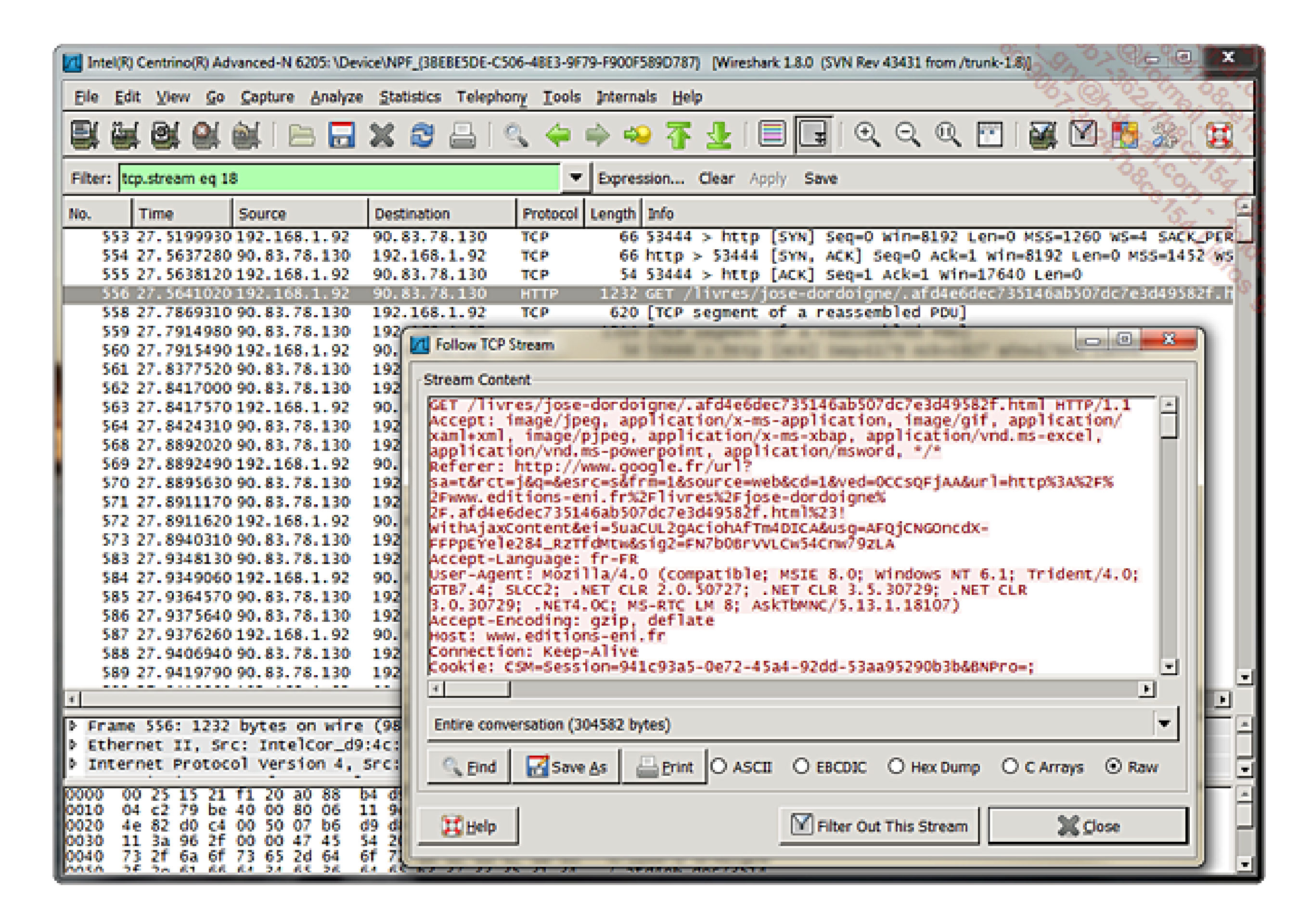


Alertas phishing en fraudwatchinternational.com

2. Escuchas de red

En el mundo del software libre, existen muchas aplicaciones. Entre ellas, WireShark ha reemplazado al célebre Ethereal. Es capaz de reconstruir una sesión TCP, es gratuito y tiene licencia GPL. La

escucha de red, o *sniffing*, es sobre todo una actividad de expertos, ya que las herramientas no sustituyen a la capacidad de interpretación.



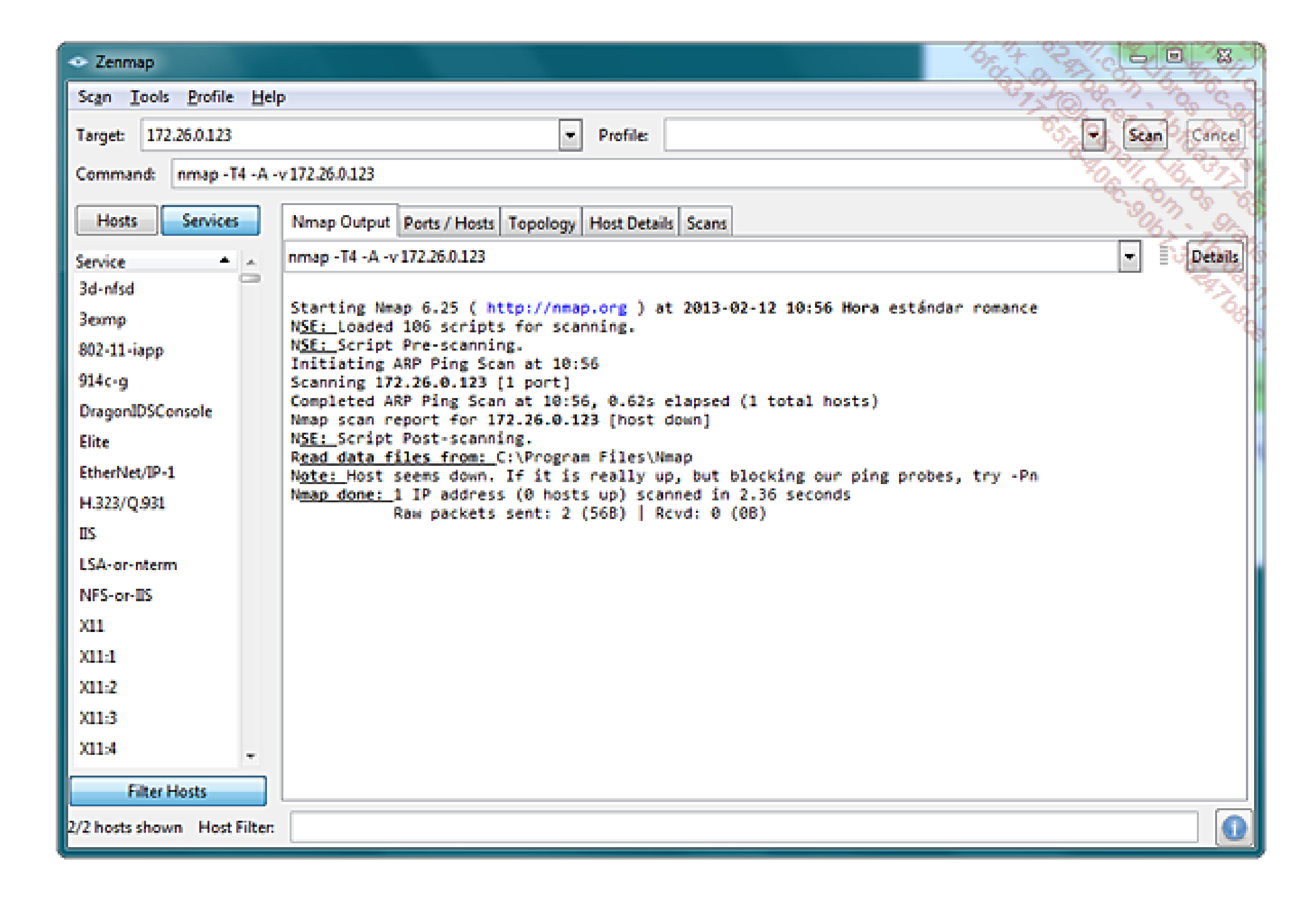
Ejemplo de seguimiento de una sesión TCP

3. Análisis de los puertos

En una red de tipo TCP/IP, un servicio escucha por un puerto, TCP o UDP, que le es propio. A cada uno corresponde un número entre 0 y 65.535. La primera serie, hasta 1024, incluye los puertos conocidos (*well known port*) de aplicaciones estándar, como:

- 80, para HTTP.
- 25, para SMTP.
- 53, para DNS.
- 21, para FTP...

El análisis de puertos consiste en recorrerlos sucesivamente. Se habla de «scan». Cuando se solicita un puerto en escucha, responde. A veces se devuelve mucha información, como se puede ver en la siguiente imagen. Este servidor Windows 2003, de prueba afortunadamente, acumula, entre otras cosas, los servicios de directorio LDAP, y las funciones de servidor HTTP y SMTP de *Internet Informations Server* (IIS). El escáner de puertos utilizado es gratuito y extremadamente fácil de utilizar.



Ejemplo de análisis con Nmap

Existen numerosos programas gratuitos disponibles en Internet, como Nmap (*Network mapper*) o SuperScan. Proponen diferentes técnicas de barrido, más o menos discretas, que permiten que la escucha sea menos activa.

4. Códigos maliciosos

Estas aplicaciones se pueden componer de dos funciones diferentes:

- La posibilidad de reproducirse.
- La posibilidad de ataque, con una carga nociva.

A menudo se designan con el nombre genérico de virus, pero realmente se les puede diferenciar. Este nombre se define claramente en la RFC 1135, que puede encontrarse en la direcciónhttp://www.ietf.org/rfc/rfc1135.txt.

Un virus es un bloque de código que se introduce en un huésped para propagarse, pero hay que ejecutarlo para que se active. Es diferente del gusano (*worm*), que se propaga por el correo electrónico o por fallos de la red. El gusano no contiene necesariamente una carga nociva. La bomba lógica, que se ejecuta condicionalmente, por ejemplo en una fecha determinada, es una tercera variación en este tema.

Estos códigos maliciosos provocan numerosos ataques. Las principales intrusiones se dan a conocer por los medios de comunicación, lo que demuestra la importancia de sus efectos.

Los códigos maliciosos disponen de dos medios importantes de propagación. El primero es seguir utilizando la credulidad de los usuarios, mediante ingeniería social. De hecho, son muchos los que no se resisten al asunto tentador de un mail que contiene un documento adjunto recibido de un remitente desconocido.

La utilización de las vulnerabilidades de las aplicaciones es la segunda vía para su transmisión. Los sistemas operativos no son los únicos afectados. Los navegadores Web Internet Explorer y Mozilla

Firefox son los más vulnerables.

5. Programas furtivos

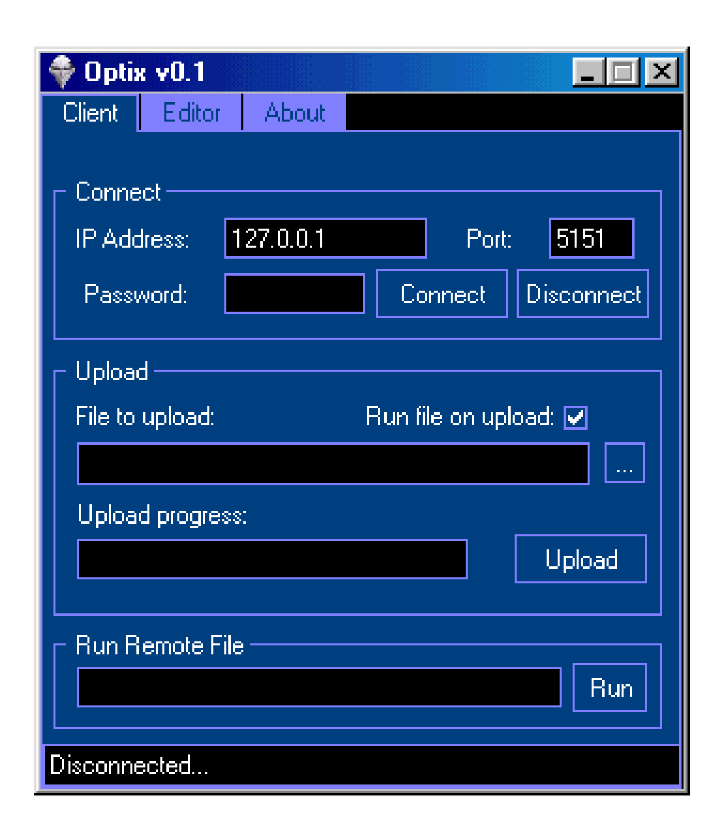
El caballo de Troya (*Trojan horse*), o troyano, podría entrar en la categoría de códigos maliciosos, pero no tiene las dos funciones de estos. Por el contrario, un gusano puede instalarlo en un ordenador.

Una vez instalado, este programa permanece oculto. Puede que su función sea simplemente abrir un puerto de red, o utilizarse como un servidor. Así, el pirata toma el control de la máquina.

Por ejemplo, podemos citar a Optix, que es un troyano. Permite a una persona maliciosa descargar y ejecutar archivos en el ordenador de su víctima.

Una vez que se ha instalado el programa, haciendo creer que se trata de un antivirus, u ofreciéndolo en un paquete más completo para que pase desapercibido, el programa se copia en la carpeta Windows y modifica el registro para ejecutarse automáticamente al arrancar el ordenador.

Una vez arrancado, abre un puerto y espera que un usuario remoto le pida realizar operaciones de transferencia de archivos o de ejecución remota por medio de la siguiente utilidad:



Ejemplo de una interfaz para manejar un troyano

El software espía, o *spyware*, es una subcategoría de caballo de Troya. Puede ser:

- Con un objetivo comercial, recogiendo datos para orientar campañas publicitarias.
- Informador, que recoge información y la envía discretamente.

En esta última categoría de software espía, los programas *keyloggers* se encargan de transmitir la información introducida por medio del teclado, como contraseñas o números confidenciales.

Los *bots*, diminutivo de robots, son software que permite controlar una máquina remota. Pasan a ser «zombies» y se pueden utilizar para lanzar un ataque programado, o servir de enlace para los ataques de *spam*. Un *bot* también permite desencadenar un informador durante un periodo determinado o ejecutar un caballo de Troya a petición.

En cualquier caso, este software trabaja de espaldas al usuario, pero también de los informáticos de

la empresa.

Conceptos de protección en la red local

1. Servicios de seguridad

Para responder a la solicitud de garantías necesarias en términos de seguridad de un Sistema de Información (SSI), estos servicios deben tener en cuenta los conocimientos y análisis efectuados.

Los distintos servicios de seguridad que se deben mantener son:

- Control de acceso al sistema.
- Gestión de permisos.
- Integridad.
- No denegación.
- Autentificación.
- Confidencialidad.

Esta protección se aplica tanto a la información como a los sistemas de soporte. Es muy importante que ninguno sea forzado ni olvidado. Aquí trataremos específicamente los dos principales que debe tener una red, la autentificación y la confidencialidad.

a. El control de acceso al sistema

Se trata, sobre todo, de proteger físicamente los dispositivos. Es necesario cerrar las salas de servidores, pero también las oficinas. De hecho, se puede robar dispositivos móviles que contienen información importante.

Los sistemas operativos y otras aplicaciones deben estar protegidos mediante la configuración e instalaciones regulares de parches que corrijan los posibles errores.

Las redes se pueden aislar y se deben filtrar las comunicaciones.

Se debe instalar y mantener software antivirus en todos los equipos. Se puede completar con la instalación de herramientas de detección de intrusión (IDS - *Intrusion Detection System*).

b. La gestión de permisos

El software, especialmente los sistemas operativos, utilizan su propio sistema de habilitación de accesos a los archivos o a los datos. Por ejemplo, Microsoft Windows utiliza los permisos NTFS, nombre tomado del sistema de archivos. Los sistemas Unix/Linux tienen una gestión basada en los accesos de lectura (*read*), de escritura (*write*) y de ejecución (*execute*). Los fallos en las distribuciones de estos permisos pueden aparecer rápidamente si no se utiliza una política conveniente.

Además, hay permisos no vinculados a los propios datos, pero sí a posibles acciones sobre aplicaciones, que deben administrarse complementariamente.

Para facilitar la gestión de los permisos, los usuarios se registran en bases de cuentas o directorios centralizados. Los derechos y permisos se asocian así a una cuenta, o a un grupo al cual pertenece esta. A continuación el usuario debe demostrar su identidad, dándose a conocer ante una cuenta conocida.

c. La integridad

Comprobar la integridad en las transferencias es asegurarse de que no tenga lugar ninguna modificación entre el emisor y el destinatario (hombre o máquina). Puede ser un muy buen

complemento de la confidencialidad.

El CRC aún es falible y cualquier pirata lo puede manipular discretamente. Pero de todos modos sigue siendo conveniente para paliar los problemas de transmisión. La aplicación de tablas de *hash*, que calculan una huella digital, sigue siendo más fiable.

Las tablas de *hash* utilizan un algoritmo de criptografía que genera un texto de longitud fija, cualquiera que sea el tamaño del de entrada. El resultado de este cálculo se llama condensado, huella o *hash*. Esta función es de dirección única, puesto que no es posible encontrar el texto de origen a partir de la huella que se comunica al destinatario. Este puede efectuar el mismo cálculo a partir del contenido de la trama enviada. Basta solo una modificación para no encontrar el mismo resultado y considerar que se ha alterado el contenido. Los dos principales algoritmos utilizados son:

- *Message Digest 5* (MD5), que genera huellas de 128 bits.
- *Secure Hash Algorithm 1* (SHA o SHA1), que genera resultados de 160 bits.

El servicio de integridad, en términos de almacenamiento y administración de los sistemas, lo pueden ofrecer los archivos históricos y las auditorías.

d. La no denegación

Este servicio lo proporciona la firma electrónica (que no es lo mismo que la autentificación). Su reconocimiento y, por tanto, su validación, implica la confianza de un tercero. Además, añade a esta validación de identidad un cálculo de integridad con tablas de *hash*.

La firma electrónica se puede utilizar en sitios Web (validación de procedencia de los datos), en mensajes de correo electrónico, en el interior de un archivo...

2. Autentificación

Este servicio de seguridad es particularmente importante cuando un hardware se conecta a una red, es decir, cuando da acceso a otras máquinas. En realidad, incluye dos funciones. La primera es la identificación, es decir, el reconocimiento de la identidad. La segunda, la autentificación, comprueba la identidad declarada.

Se pueden utilizar cuatro formas de comprobación:

- «Lo que conozco», como contraseña.
- «Lo que tengo», como soporte físico.
- «Lo que soy», examinando una característica humana.
- «Lo que sé hacer», como una firma manuscrita.

En la autentificación informática, este último caso requiere una pantalla táctil. Por lo tanto, no lo trataremos en esta obra.

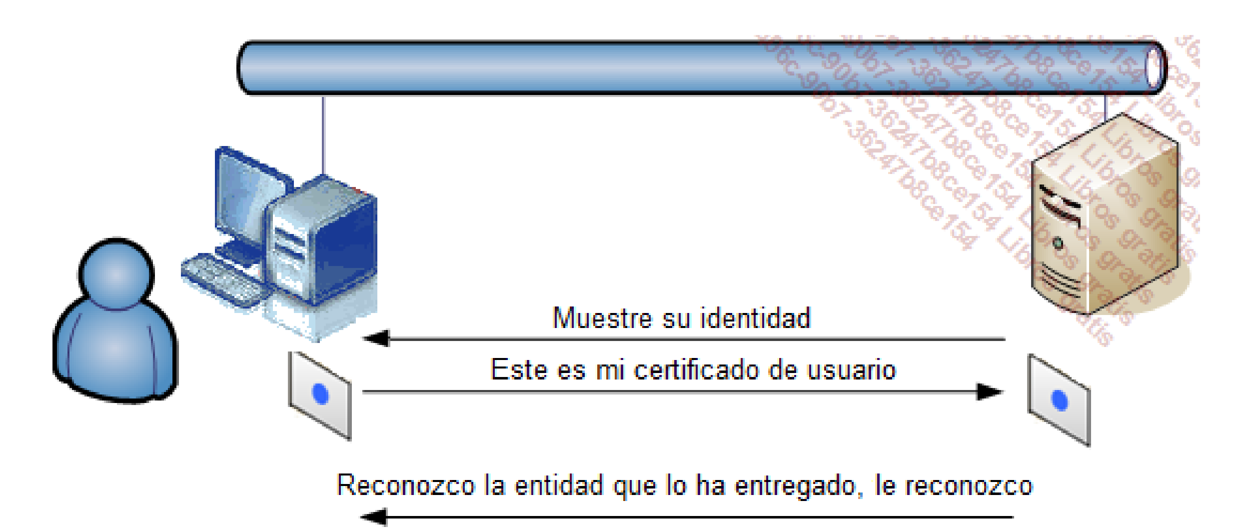
Cuando el alcance de una red va más allá de los edificios controlados, a través de Internet o por las ondas hertzianas, hay que hacer una reflexión sobre la elección del medio de autentificación. Existen soluciones, más elaboradas que la habitual contraseña, y de bajo coste, que reducen los riesgos de suplantación de identidad.

a. La identificación

El principal medio de identificación es el «login». El usuario lo introduce y se controla en una base de datos o un archivo.

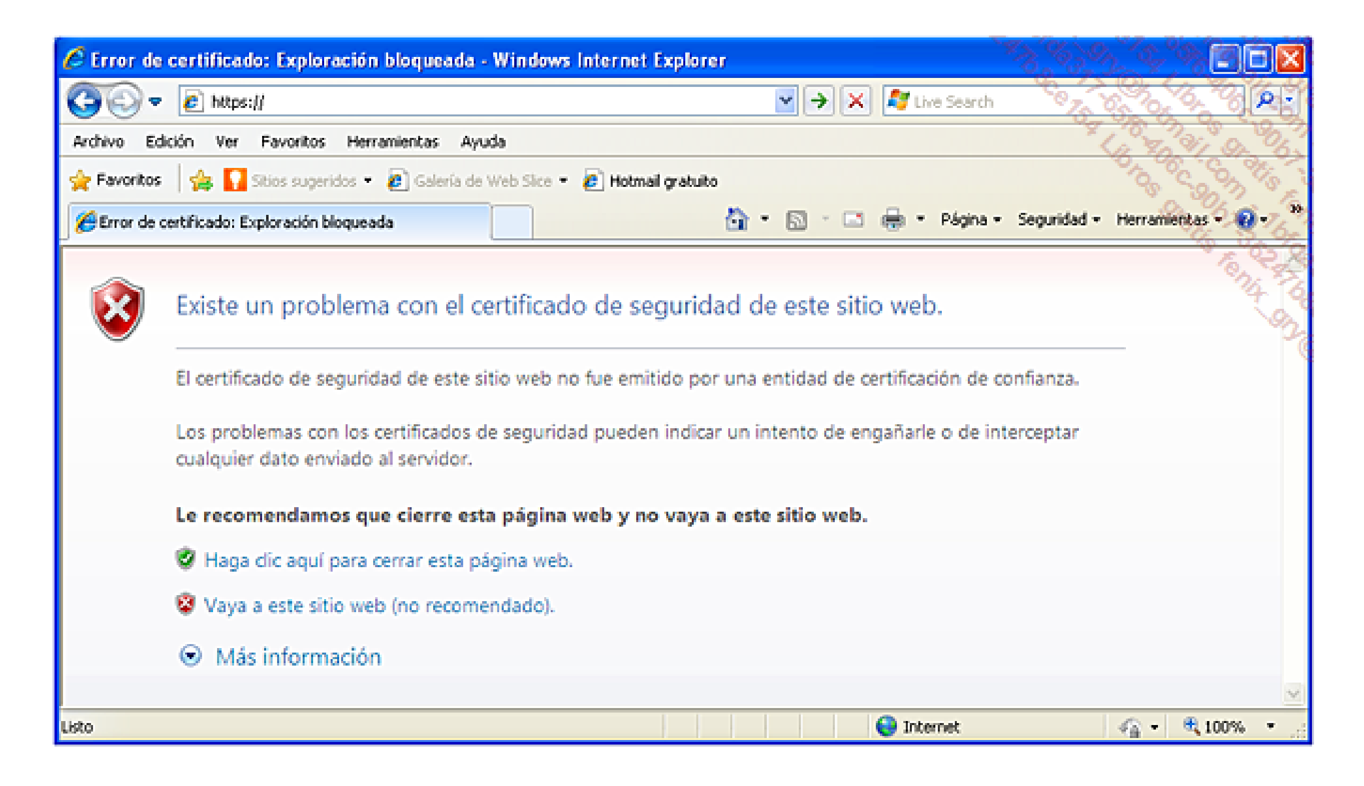
La informática permite, como en otros aspectos de la vida, el uso de una especie de carnet de identidad, el certificado electrónico, que debe ser reconocido por todos los sistemas, y, por tanto,

su formato es estándar. El actual es X509, en su versión 3. A petición de uno de los extremos de la comunicación, el otro presenta su certificado para justificar su identidad.

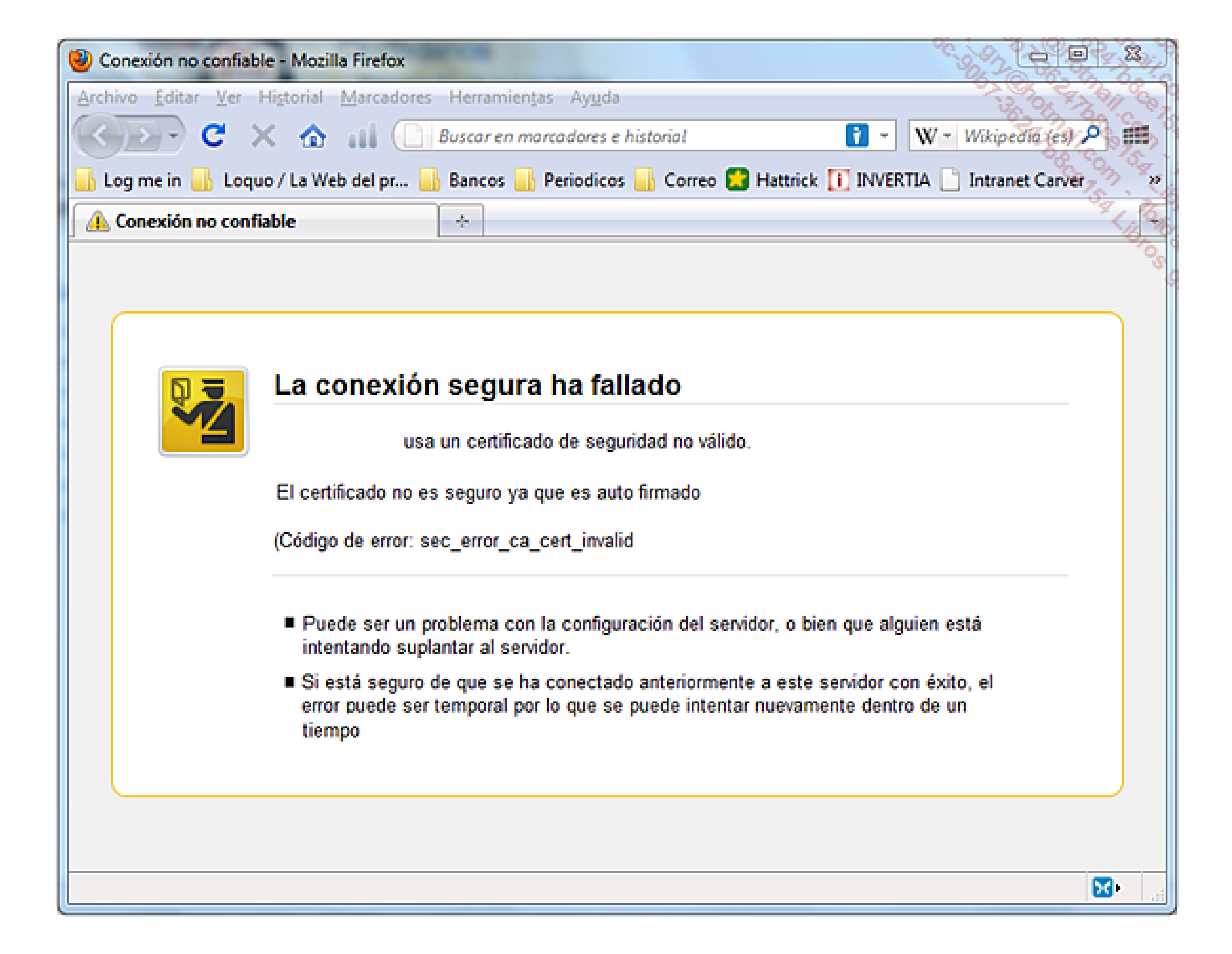


Una entidad entrega un certificado electrónico: la autoridad de certificación (CA - *Certificate Authority*) o una de sus delegaciones. El ordenador que pide la comprobación debe conocer a esta entidad. Esta autoridad es la garantía de confianza.

Si no se reconoce la autoridad de certificación, aparece un mensaje explícito en el navegador (en los navegadores de nueva generación). En caso de no reconocimiento de la autoridad de certificación, esta página sustituye al cuadro de diálogo que conocemos.



Certificado no reconocido en MS IE7

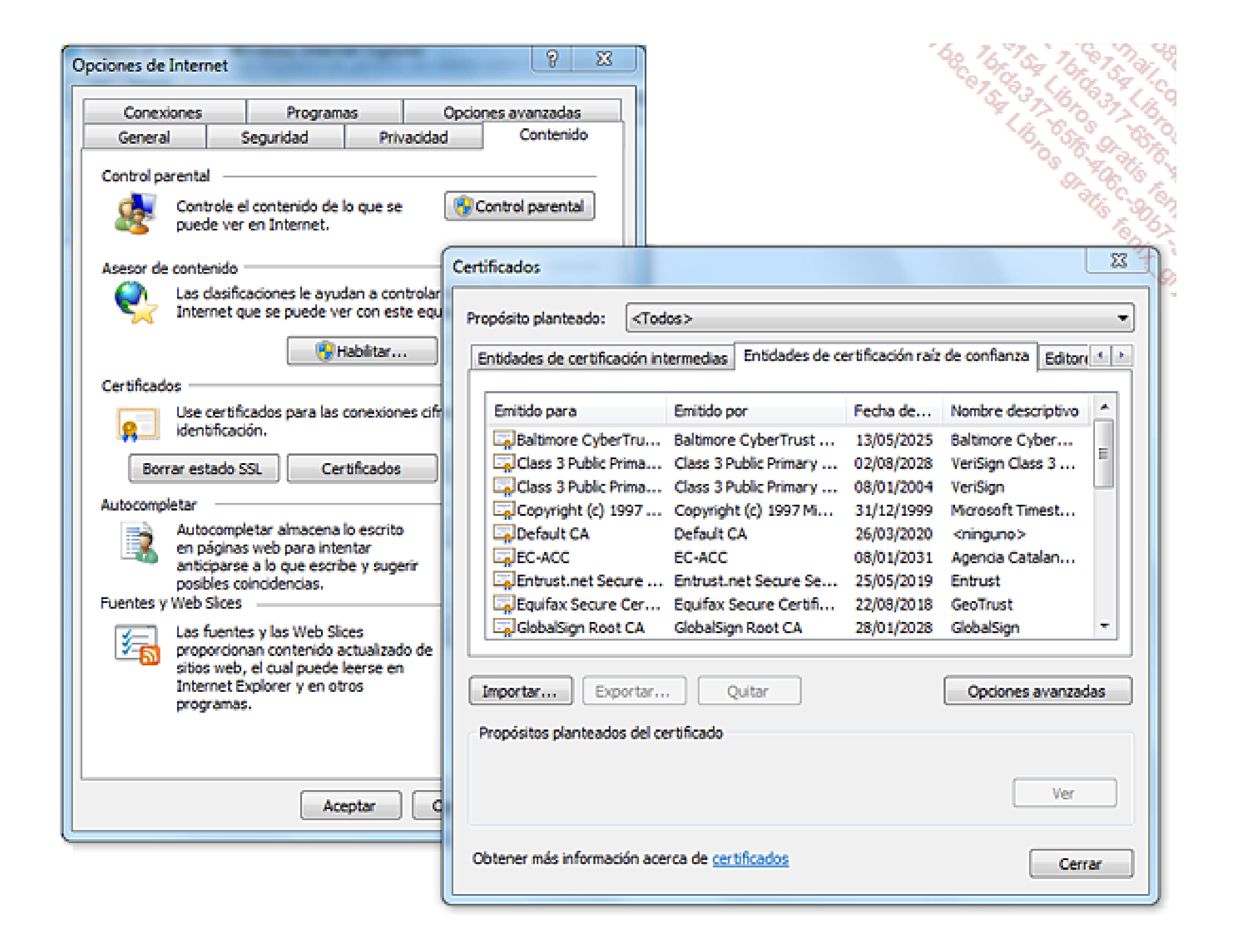


Certificado no reconocido en Firefox 3

Una empresa puede poner en marcha sus propios servidores de entrega y gestión de certificados. Este sistema es la infraestructura de gestión de claves (PKI - *Public Key Infrastructure*), ya que, y lo veremos más adelante, la gestión de las identidades solo es una de sus funciones.

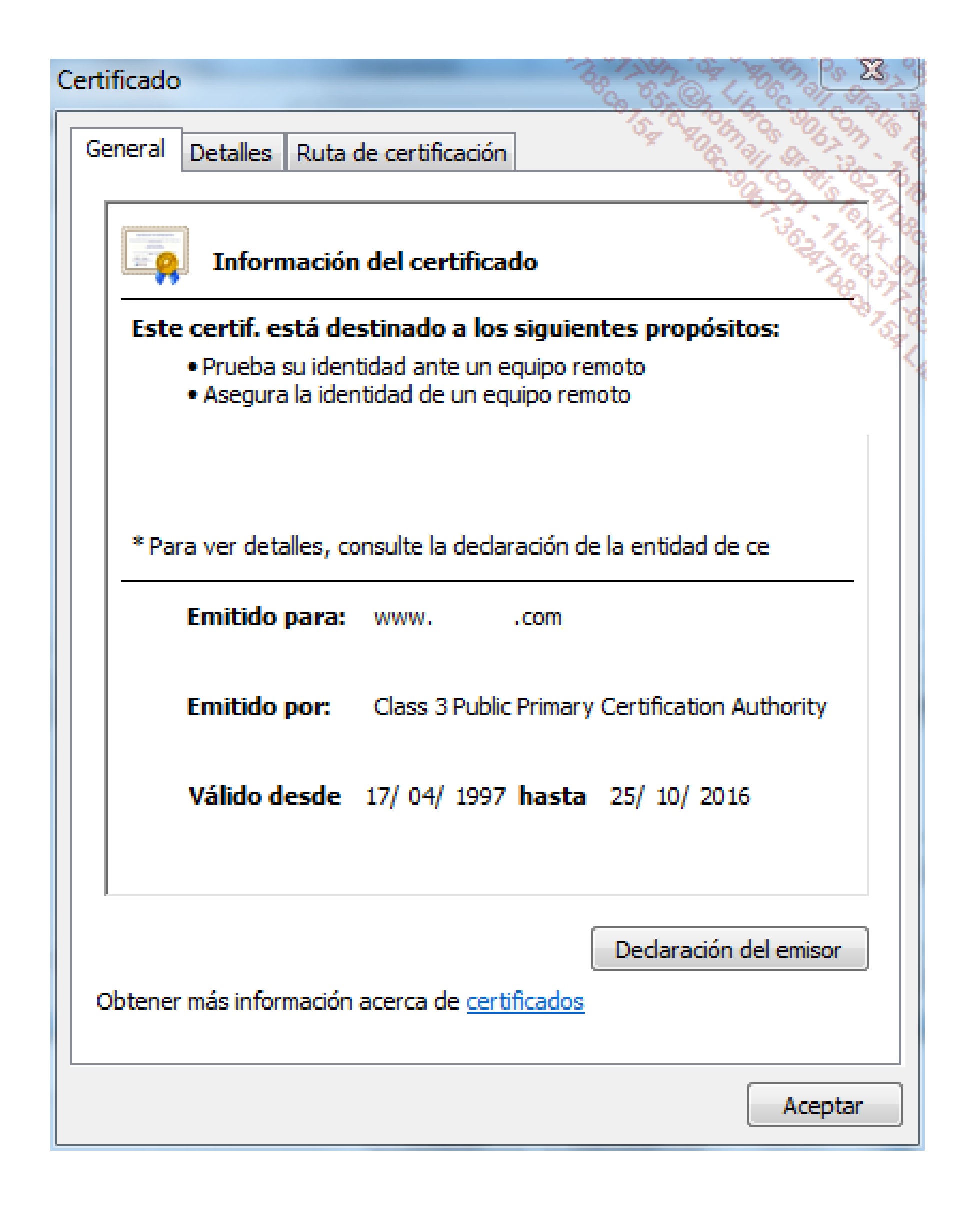
Para evitar el despliegue y la administración de esta infraestructura, los certificados se pueden comprar a empresas especializadas. Están reconocidas a nivel mundial.

Se debe reconocer la identidad justificada por el certificado. Para esto, es necesario, en primer lugar, que la autoridad que entrega el certificado esté reconocida por el sistema que la comprueba. En los sistemas Windows, por ejemplo, están enumeradas en las propiedades de Internet Explorer, en la ficha **Contenido**. Si se despliega una infraestructura de gestión de claves para la empresa, es necesario que todos los equipos y servidores interesados la reconozcan.



Raíces de confianza en IE8

Los certificados electrónicos pueden justificar la identidad de un usuario o de un servidor. También tienen otras aplicaciones.



b. La autentificación por contraseña

La contraseña actualmente representa el medio de autentificación más común.

La primera categoría es la contraseña estática. Se trata de una simple secuencia de caracteres alfanuméricos y especiales, elegidos por el usuario, y por un periodo que puede ser limitado o ilimitado. Para comprobar su introducción, se almacena en un archivo o una base de datos en el ordenador o en un servidor. Esta contraseña puede ser objeto de diversos ataques para intentar obtenerla, por ingeniería social, diccionario o fuerza bruta.

El uso de contraseñas dinámicas reduce la debilidad de la autentificación. Entre las técnicas utilizadas, la más usual combina el conocimiento del código de autentificación con un soporte físico. Cada contraseña, también llamada testigo (*Token*), se puede usar una sola vez (OTP -*One Time Password*). Se ofrece al usuario por medio de un generador, la tarjeta de testigo, que la calcula aleatoriamente. Se incluye un factor temporal para hacerla única. También es necesario el correspondiente componente informático en el servidor para que valide esta contraseña. La solución más conocida de este tipo es RSA, de Secure ID, cuyo modelo de tarjeta de testigo es el que se ve a continuación:



En cuanto a su implementación, esta solución es un poco más compleja que la anterior. Además, requiere la sincronización regular de la tarjeta de testigo con el servidor. Es muy difícil que falle, mientras no roben el componente físico o no se pierda. El acceso a este se puede proteger con un código.

c. La autentificación con soporte físico

Ya hemos visto que las soluciones de contraseña dinámica pueden recurrir a un soporte físico. Pero este dispositivo se puede utilizar en una sola solución de autentificación. En este caso, es necesario el reconocimiento del objeto a distancia o por inserción en un lector. Este medio es mucho más seguro que el uso de una contraseña estática y resulta más sencillo que la solución con contraseña dinámica.

El soporte físico puede ser una tarjeta inteligente. Su accesibilidad lógica requiere además el conocimiento de un código, el *Personal Identification Number* (PIN). Muy utilizado en tarjetas de crédito, o en el *Subscriber Identity Module* (SIM) de la telefonía móvil.

Una tarjeta inteligente requiere un lector específico. Ofrece una pequeña capacidad de memoria y puede contener contraseñas, o incluso el certificado de identidad de su dueño.

Un segundo soporte puede ser una llave USB especial. Al contrario que la solución anterior, el conector, presente en todos los ordenadores modernos, permite leer su contenido. Este medio también ofrece más capacidad de memoria para el almacenamiento de información personal. Su acceso puede estar protegido por una contraseña o incluso por reconocimiento de la huella dactilar.



d. La autentificación por biometría

Una huella dactilar es una característica biométrica. Permite comprobar directamente la identidad de la persona y no requiere nada más, ni código PIN, ni contraseña. Se trata del medio más sencillo y seguro para el usuario. De hecho, ¡el usuario siempre lleva el identificador con él y es muy difícil de robar!

En contraposición, el acceso biométrico es un poco más complejo y requiere dispositivos más costosos. La huella dactilar es el mecanismo más sencillo, más utilizado que soluciones como el reconocimiento de voz o la lectura del iris.

La comprobación de la singularidad de las características del dedo es muy accesible; para ello se utilizan lectores específicos o incorporados al teclado, al ordenador portátil o al dispositivo móvil.

En contrapartida, esta autentificación no permite una disponibilidad permanente a determinada información, que se almacena en tarjetas inteligentes y llaves USB.



Los dispositivos generalmente no permiten la lectura de la huella dactilar poniendo el dedo encima. De hecho, la huella se podría recuperar si se marcase así sobre el lector. Como vemos en las fotografías anteriores, los dispositivos necesitan que se deslice el dedo sobre un escáner.

3. Confidencialidad

Hacer secreto un mensaje es la primera función de los sistemas de criptografía. Para esto se realiza una transformación, llamada codificación, de la información confidencial, el texto sin protección. El resultado es un texto cifrado o criptograma. El texto original se encuentra normalmente a través de una operación de descifrado.

Con frecuencia se utiliza la expresión encriptación en lugar del término cifrado.

En informática, las funciones matemáticas, los algoritmos criptográficos, generan claves que pueden servir para los cálculos de cifrado o descifrado.

Realizar un desencriptado es intentar encontrar el texto desprotegido a partir de un criptograma, sin conocer la clave de descifrado. Esta acción se cataloga como análisis criptográfico.

La necesidad de confidencialidad en el intercambio de información es aún más importante en las redes abiertas. Si el paquete no debe leerse cuando viaja entre el emisor y el receptor, es necesario cifrarlo, para que circule transparente. Esto se puede realizar en las capas bajas, medias o altas del modelo de red.

En términos de almacenamiento, si una información se considera confidencial, se debe cifrar el archivo que la contiene. Esta acción de cifrado se recomienda particularmente en dispositivos portátiles y móviles.

Se utilizan dos familias de sistemas criptográficos para hacer confidenciales las comunicaciones de red. Emplean:

- Claves simétricas, utilizadas a la vez para el cifrado y el descrifrado.
- Claves asimétricas (privadas/públicas), utilizadas cada una para una de las dos tareas.

a. El cifrado con claves simétricas

Este método es el más antiguo. Se utiliza una sola y única clave generada por un algoritmo. Es necesaria tanto para la operación de cifrado como para la de descifrado.

Esta clave, que tiene que ser secreta, debe transmitirse siempre entre el emisor y el destinatario. Se trata del principal problema del uso de este sistema.

La fiabilidad del intercambio de mensajes cifrados por clave simétrica depende de dos factores:

- El tamaño de las claves.
- Su frecuencia de renovación.

Es necesaria una correspondencia equilibrada entre la longitud de la clave y la potencia de cálculo solicitada. De hecho, si la clave es demasiado pequeña, se puede descubrir fácilmente y los paquetes pierden su confidencialidad. Si es muy grande, los cálculos de cifrado/descifrado pueden necesitar una capacidad de procesador incompatible con las necesidades de otras comunicaciones simultáneas o la utilización de dispositivos poco potentes (PDA, *smartphone*...).

Se asigna manualmente una clave estática, tanto en el emisor como en el receptor. En este caso, se puede determinar que no se renueve la clave. Esto aumenta las oportunidades que tiene un pirata de encontrarla. Es preferible el uso de métodos de utilización de claves dinámicas, es decir, renovadas regularmente.

Los algoritmos de cifrado simétricos más utilizados son:

- *Rivest's Cipher* n°4 (RC4), que utiliza claves de diferentes tamaños, generalmente hasta 256 bits.
- *Data Encryption Standard* (DES), cuyas claves son de 56 bits.
- Triple DES, variante del algoritmo anterior, que calcula sucesivamente con 3 claves DES, dos de ellas diferentes.
- *Advanced Encryption Standard* (AES), el más reciente, con claves de 256 bits.

b. El cifrado de claves asimétricas

Complementaria a la técnica de clave simétrica, esta utiliza dos claves distintas:

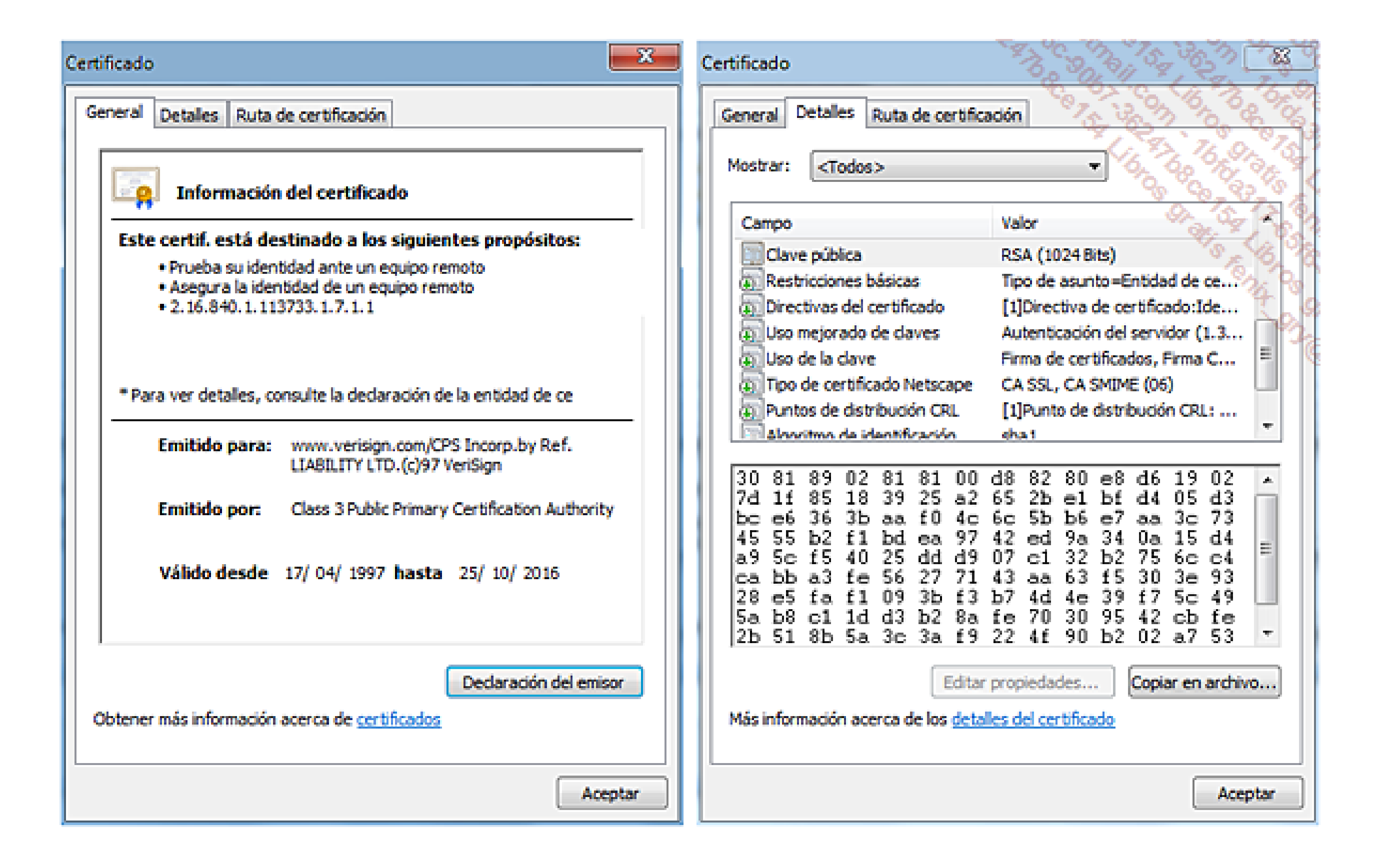
- La primera, privada, tan solo la conoce su propietario.
- La segunda, pública, que es la que se transmite.

Estas dos claves están relacionadas matemáticamente, lo que hace una solo puede deshacerlo la otra. En cambio, no es posible encontrar una por medio de la otra. Si se hace un cifrado con la clave pública, solo la clave privada correspondiente, que está protegida permanentemente, puede descifrar el mensaje.

Este método asimétrico implica no tener que generar sistemáticamente un nuevo par de claves. Eso implicaría complicaciones de administración y gestión de claves. Se prefiere que la clave tenga una vida más larga, lo que conlleva unos tamaños de clave más grandes que antes.

La utilización de cifrados asimétricos generalmente requiere la implementación de una infraestructura de gestión de claves (PKI - *Public Key Infrastructure*), como la que se utiliza para la identificación. De hecho, hay que identificar al dueño de la clave pública. Por eso se añaden las características al certificado, que igualmente tiene la clave pública que se ha de utilizar.

En la siguiente impresión de pantalla, vemos que al fabricante se le asocia una clave pública.



Las claves privadas se almacenan en una parte no pública del certificado.

Los certificados electrónicos también proporcionan en su parte pública el algoritmo de tabla hash utilizado para comprobar la integridad de los paquetes entregados.

El algoritmo de cifrado asimétrico más utilizado es Rivest, Shamir, Adelman (RSA), del nombre de sus tres creadores, que compite con el Diffie-Hellman. Las claves utilizadas tienen generalmente tamaños de 1024 o 2048 bits, o incluso superiores.

Para las comunicaciones de red, el cifrado con estas claves de todos los mensajes implicaría potencias de cálculo muy importantes. Es más bien la clave simétrica de cifrado la que se protege al viajar con un sistema asimétrico. A partir del momento en que cada entidad posee una clave, se puede implementar un túnel de cifrado. De hecho, la comunicación no será comprensible para cualquier otro sistema.

Secure Socket Layer (SSL), cuya versión 3 se estandariza como *Transport Layer Security* (TLS), funciona así. Este protocolo de protección de transacciones se utiliza, por ejemplo, en las comunicaciones Web efectuadas por *HyperText Transfer Protocol Over TLS* (HTTPS). La implementación de esta seguridad se desarrolla del siguiente modo.

El servidor Web proporciona en primer lugar su certificado, que el cliente debe reconocer. Este último genera una clave de cifrado simétrico, cifrada a su vez con la clave pública proporcionada por el certificado. Luego, esta información se reenvía al servidor, que puede encontrar la clave simétrica gracias a su clave privada. A continuación, toda la comunicación está cifrada dentro de un túnel seguro.





Esta es mi identidad y mi clave pública

De acuerdo, esta es la clave de cifrado,
que está cifrada con su clave pública

Comunicación dentro de un túnel de seguridad

4. Protección de los datos de usuario

Uno de los principales problemas en materia de seguridad es la protección de los datos sensibles de la empresa. Estos datos están en manos de los usuarios.

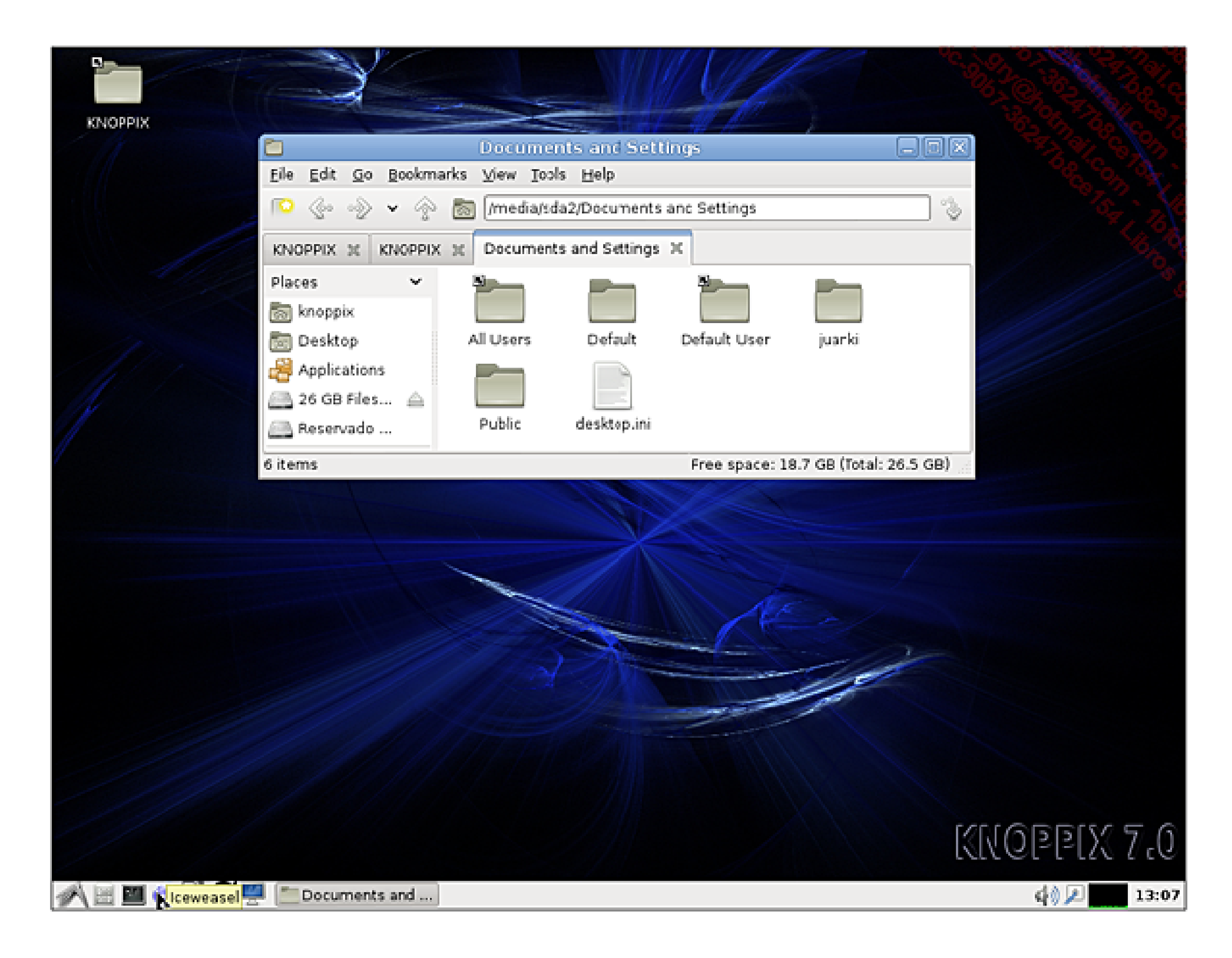
A menudo, la empresa no tiene otra opción que permitir al usuario trabajar localmente con estos datos en dispositivos móviles como ordenadores portátiles.

Casi siempre, la primera protección del equipo es únicamente una contraseña de administrador que nadie conoce.

Desafortunadamente, si el acceso como administrador a menudo no es posible cuando se arranca el equipo de manera normal, no sucede lo mismo cuando se utiliza algún otro sistema de tipo «Live CD» para arrancar el ordenador. Es entonces cuando se toma conciencia de que la seguridad de los datos del ordenador es mínima.

> Un «Live CD» es un sistema operativo en un soporte removible que arranca completamente sin instalar nada en el disco duro del ordenador.

De este modo, si se arranca un equipo con Windows 7 formateado en NTFS, con una versión de Knoppix de Linux, se accede fácilmente al contenido del disco Windows:



Acceso a una partición de Windows a partir de un Live CD Linux

Dispone de información complementaria sobre Knoppix en la URL: http://knoppix.net/

Atención, no se trata de juzgar aquí tal o cual sistema operativo. Es muy fácil recuperar una contraseña de administrador en un sistema UNIX/Linux que tenga una seguridad normal. Sin embargo, es necesario acceder físicamente a la máquina. Es por esta razón por lo que una sala de servidores tiene que estar protegida como una caja fuerte.

Por tanto, es fácil imaginar un robo de datos, a partir a partir del momento en que le roben su portátil.

Existen igualmente otros «Live CD» que ofrecen dar otro paso más y crear un nuevo acceso como administrador.

Veamos qué ofrece Microsoft por su parte.

a. Protección de la inicialización del disco

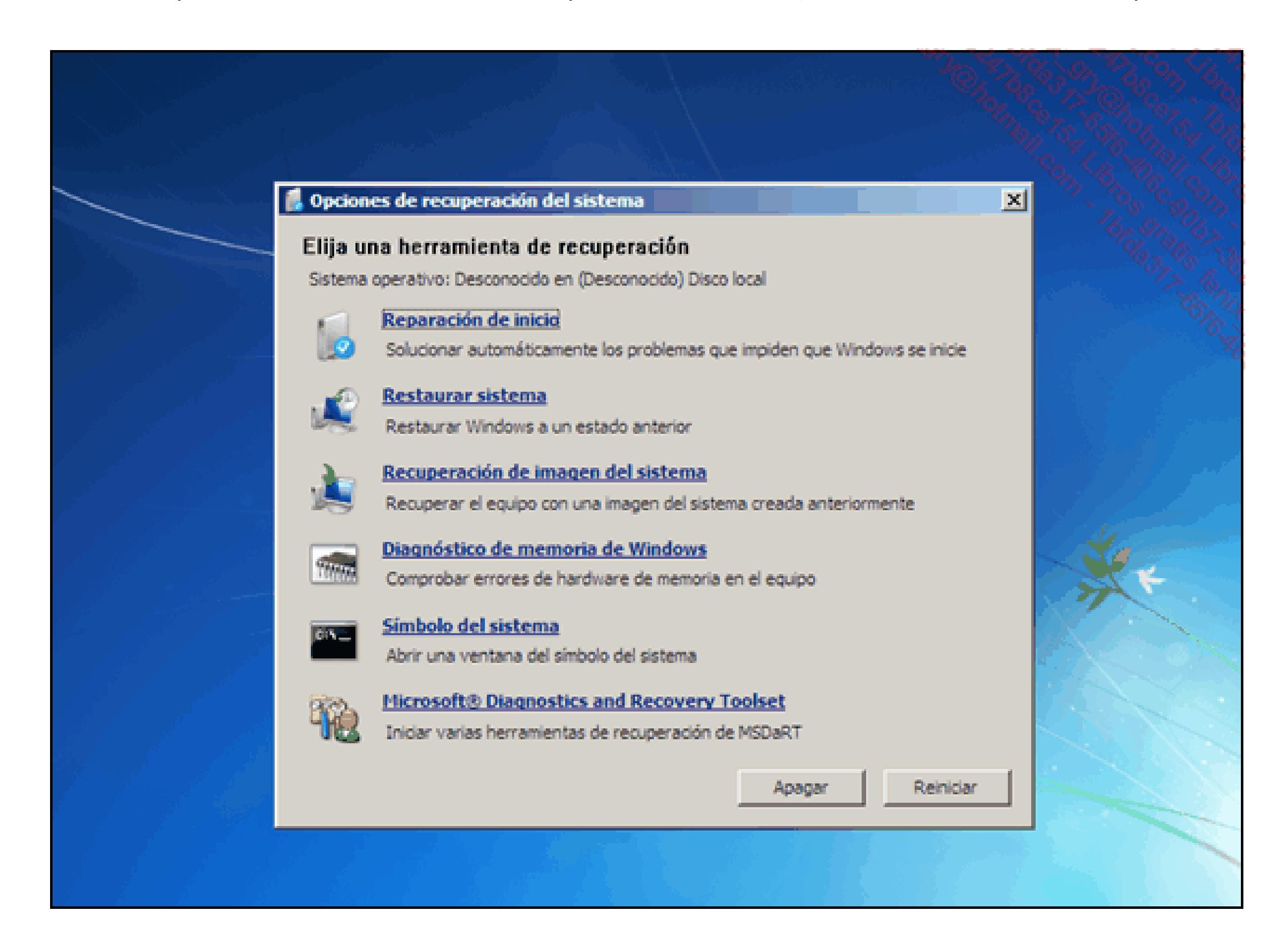
Acceso como administrador a un ordenador

Microsoft ofrece MDOP (*Microsoft Desktop Optimization Pack*), un conjunto de herramientas para empresas que han suscrito un contrato de licencias para sus equipos: este pack de optimización de los equipos integra numerosas herramientas y permite acceder a funcionalidades bajo licencias complementarias.

Dispone de más información sobre Microsoft Desktop Optimization Pack enhttp://technet.microsoft.com/es-es/windows/microsoft-desktop-optimization-pack.aspx

Así, usted puede crear discos autónomos que permiten reparar problemas en los equipos de trabajo.

Cuando arranque con el disco del sistema operativo utilizado, se le ofrecen diversas opciones:



Acceso a diferentes herramientas de reparación

Entre estas herramientas, encontramos **MSDaRT** o **Microsoft Diagnostics and Recovery Toolset**, que integra **Emergency Repair Disk Comander**.



Herramientas ofrecidas por Microsoft DaRT

Se proporcionan numerosas herramientas interesantes, entre las que destaca **Locksmith**, que permite crear una nueva contraseña de administrador.



Ejecución de Locksmith

Del mismo modo, existen herramientas de Linux que permiten reiniciar la contraseña de administrador local. La interfaz no es siempre muy amigable.

```
********************************************************************************
*                                                                              *
*       Windows Reset Password / Registry Editor / Boot CD                     *
*                                                                              *
*  (c) 1998-2011 Petter Nordahl-Hagen. Distributed under GNU GPL v2            *
*                                                                              *
* DISCLAIMER: THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTIES!               *
*             THE AUTHOR CAN NOT BE HELD RESPONSIBLE FOR ANY DAMAGE            *
*             CAUSED BY THE (MIS)USE OF THIS SOFTWARE                          *
*                                                                              *
* More info at: http://pogostick.net/~pnh/ntpasswd/                            *
* Email       : pnh@pogostick.net                                              *
*                                                                              *
* CD build date: Wed May 11 20:16:09 CEST 2011                                 *
********************************************************************************

Press enter to boot, or give linux kernel boot options first if needed.
Some that I have to use once in a while:
boot nousb          - to turn off USB if not used and it causes problems
boot irqpoll        - if some drivers hang with irq problem messages
boot vga=ask        - if you have problems with the videomode
boot nodrivers      - skip automatic disk driver loading

boot: _
```

Ejemplo de herramienta de Linux para reiniciar una contraseña Windows

Basta con elegir las opciones que se ofrecen por defecto para reiniciar la contraseña de administrador:

```
<>========<> chntpw Main Interactive Menu <>========<>
Loaded hives: <SAM> <SYSTEM> <SECURITY>
  1 - Edit user data and passwords
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] ->

===== chntpw Edit User Info & Passwords ====

| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrateur                 | ADMIN  | dis/lock |
| 01f5 | Invit                          |        | dis/lock |
| 03e9 | jose                           | ADMIN  |          |
| 03e8 | win7                           | ADMIN  |          |

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrateur]
RID     : 0500 [01f4]
Username: Administrateur
fullname:
comment : Compte dutilisateur dadministration
homedir :

User is member of 1 groups:
00000220 = Administrateurs (which has 3 members)

Account bits: 0x0211 =
[X] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total  login count: 1

 - - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
 4 - Unlock and enable user account [probably locked now]
 q - Quit editing user, back to user select
Select: [q] > 1
```

Reinicio de una contraseña de administrador

Ahora se entiende bien que nuestro sistema operativo, a día de hoy, es vulnerable.

Afortunadamente existen soluciones para fortalecer la seguridad.

En primer lugar, el hecho de poder arrancar el ordenador desde una unidad removible es un fallo de seguridad evidente.

Conviene, pues, proteger con contraseña la BIOS del ordenador para impedir cualquier modificación del arranque y configurar el arranque solo a partir del disco duro local.

Algunas empresas bloquean la utilización de dispositivos USB o solo autorizan algunos que estén homologados.

Vemos que se puede actuar a diferentes niveles:

- Protección del acceso a la BIOS.
- Control de acceso o de utilización de dispositivos móviles.
- Control del arranque del ordenador.
- Protección de datos o, lo que es lo mismo, la protección de las particiones que tienen los datos para convertirlas en inexpugnables si se arranca con otro sistema.

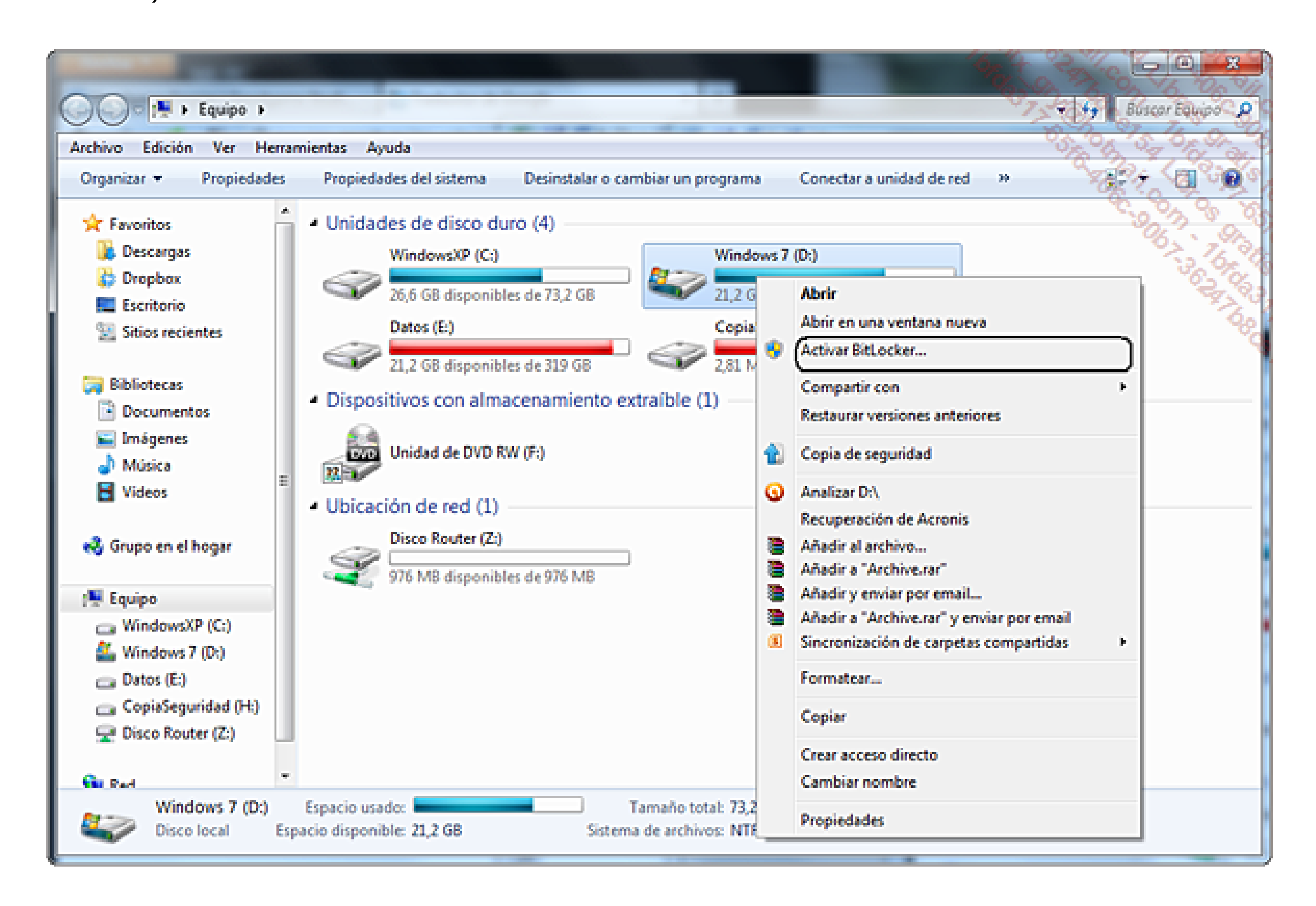
b. Cifrado de los discos locales

Ahora, examinemos las posibles soluciones para proteger los datos sensibles de la empresa.

Cifrado nativo de Windows

Actualmente, la mayoría de los equipos ejecutan Windows. Desde Windows Vista y la siguiente versión ofrecida (solo en Ultimate y Enterprise), es posible activar el cifrado de unidad BitLocker (*BitLocker Drive Encryption*) si el ordenador dispone de una tarjeta TPM (*Trusted Platform Module* o módulo de plataforma de confianza).

Esto va a permitir cifrar todo el disco de sistema e igualmente los discos de datos (locales o removibles).



Activación de BitLocker en la partición de sistema en Windows 7

BitLocker permite cifrar todo el disco, asegurando así protección para el sistema y los datos que están almacenados. Asimismo, garantiza la integridad del sistema.

Una vez se ha activado la protección, cualquier archivo grabado se cifra automáticamente. En modo de funcionamiento normal, los archivos se descifran sobre la marcha de manera transparente. Además, si el sistema se modifica, el equipo se bloquea automáticamente.

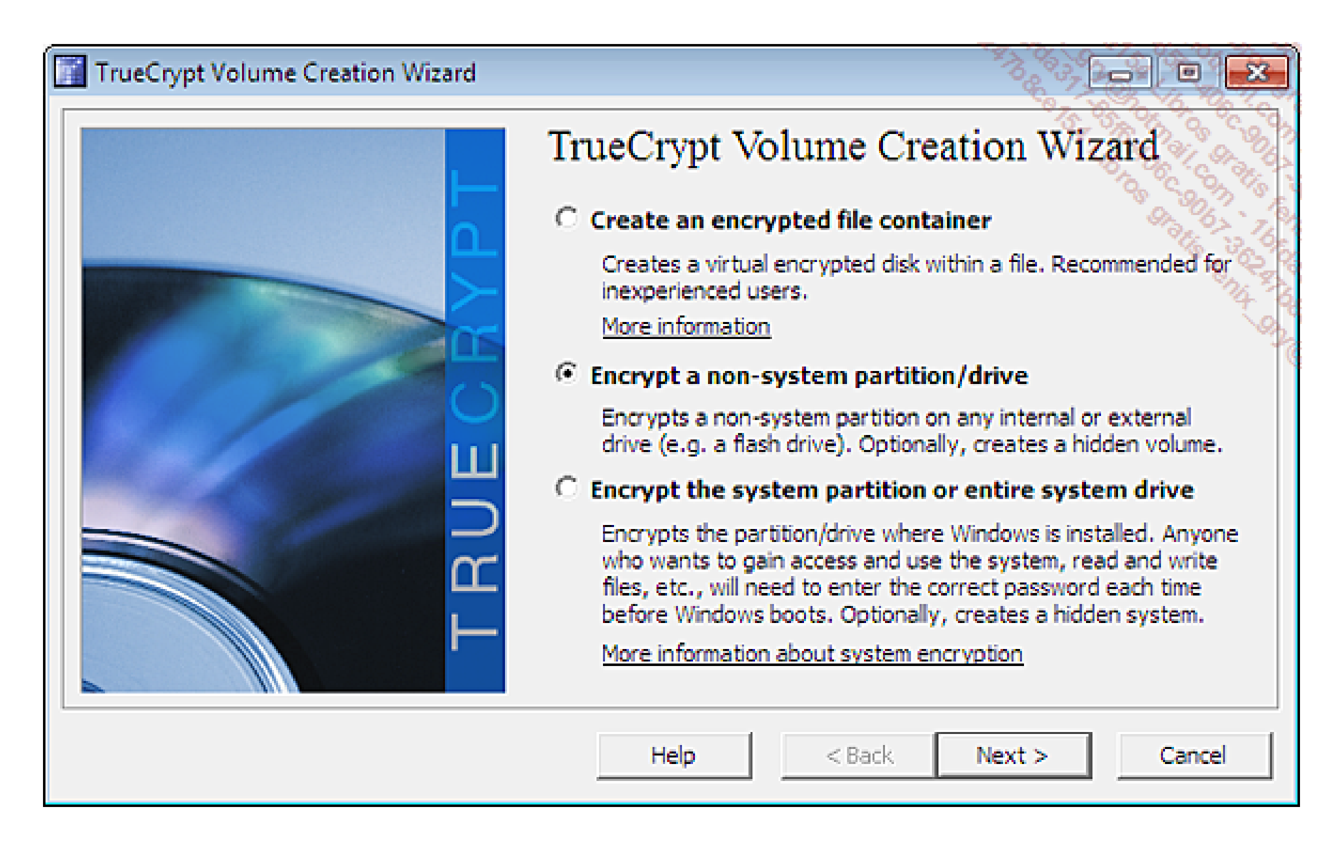
Cifrado con una solución de terceros

Existen muchas soluciones que permiten implementar el cifrado de disco.

En particular, TrueCrypt, que es una aplicación de código abierto ampliamente reconocida.

Dispone de más información en: http://www.trucrypt.org

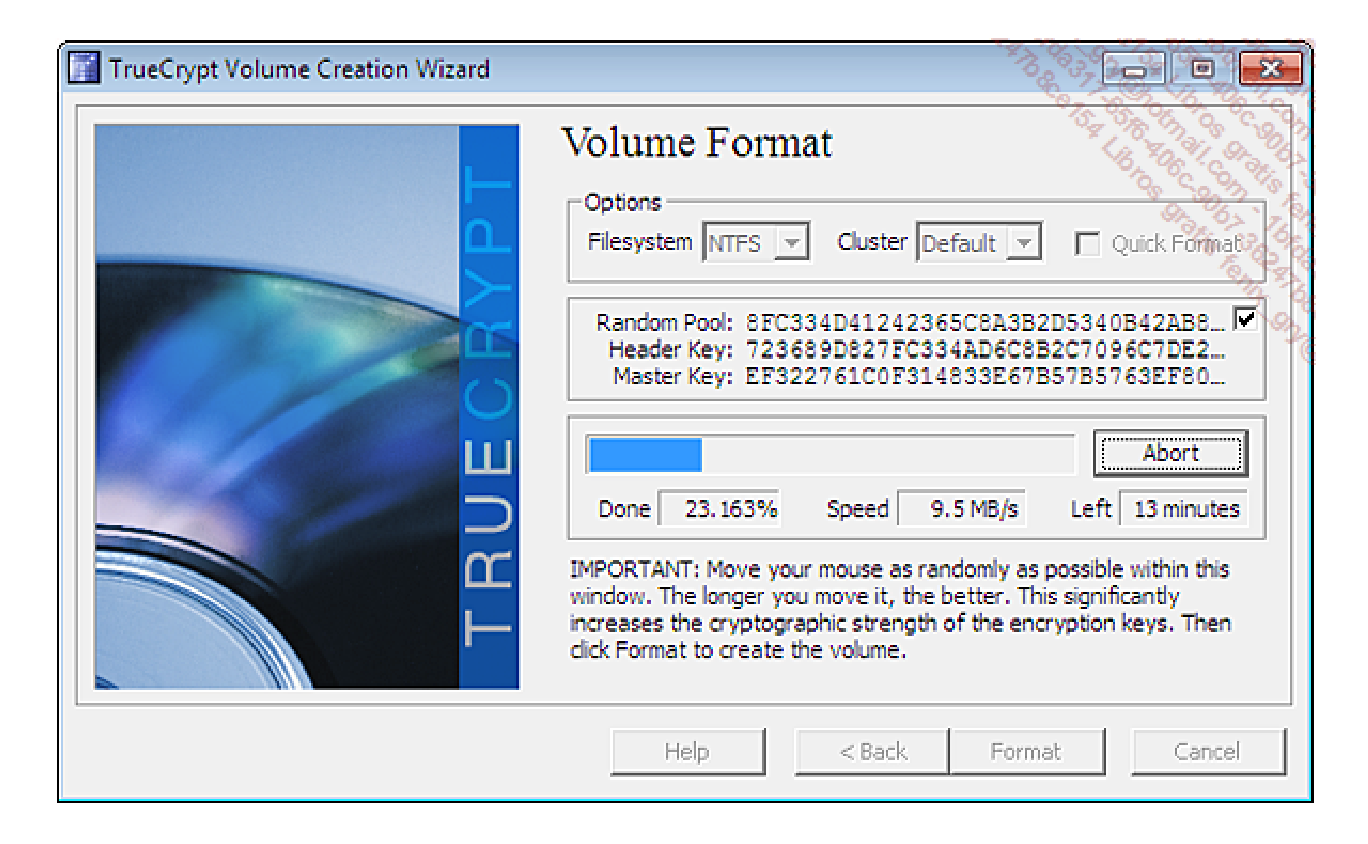
Por ejemplo, para activar el cifrado de una partición del sistema, después de haber instalado TrueCrypt y haber creado la estructura inicial de almacenamiento de las claves (el contenedor), vamos a proceder de la siguiente manera:



Cifrado de un disco de datos con TrueCrypt

Ahora hay disponibles varias opciones. Elegimos activar el cifrado al mismo tiempo que el formateo de la partición, que está en blanco.

Igualmente podríamos activar el cifrado en segundo plano para conservar los datos existentes en la partición de datos.



Formateo de una nueva partición con activación del cifrado TrueCrypt

Una vez se ha cifrado la partición, la debemos montar con TrueCrypt para poder utilizarla.

c. Cifrado de discos USB

El cifrado de discos USB se puede implementar con la tecnología BitLocker To Go o «cifrado BitLocker portable».



Cifrado de un disco USB externo en Windows 7

Cifrado de unidad BitLocker (G:)

Elija cómo desea desbloquear la unidad

Usar una contraseña para desbloquear la unidad

Las contraseñas deben contener mayúsculas y minúsculas, números, espacios y símbolos.

Escriba la contraseña: ••••••••••••

Vuelva a escribir la contraseña: ••••••••••••

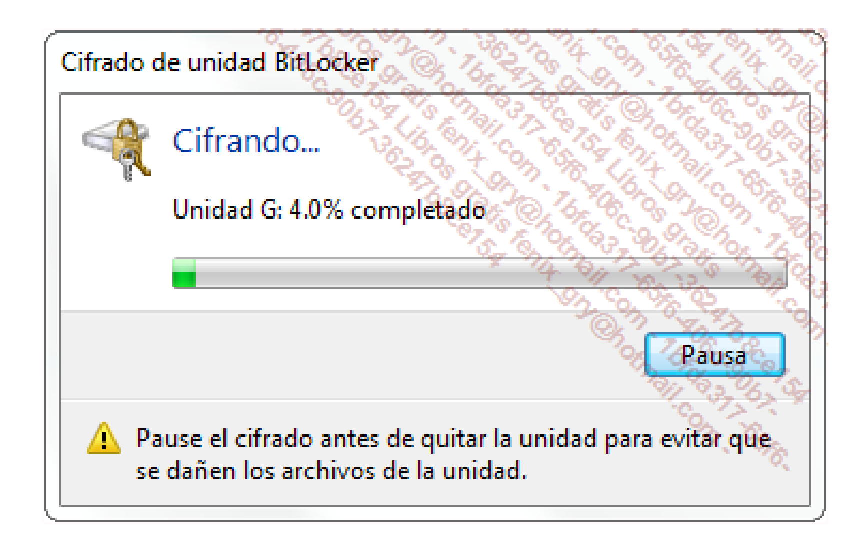
Usar la tarjeta inteligente para desbloquear la unidad

Deberá insertar la tarjeta inteligente. El PIN de la tarjeta inteligente será necesario cuando desbloquee la unidad.

¿Cómo se usan estas opciones?

Siguiente Cancelar

Definición de una contraseña para el cifrado BitLocker



Cifrado de un disco con BitLocker To Go

Protección de la interconexión de redes

Es muy raro que la red local de una empresa esté aislada. Su interconexión con Internet o cualquier otra red es algo normal. Por ello es necesario proteger las entradas y salidas de la red interna privada. Se pueden instalar diferentes equipos que se ocupen de esta protección.

1. Router de filtrado

Los mecanismos de filtrado que se pueden asociar a un router permiten el análisis de la capa 3 (de red) del modelo OSI.

El análisis de los paquetes entrantes y salientes se realiza, por ejemplo, en la cabecera IP, lo que permite acciones como:

- Bloqueo de direcciones IP (origen y destino).
- Prohibición de transmisión de protocolos de capa de Red o de Transporte utilizados (UDP, TCP o ICMP).

Algunos equipos incluyen las cabeceras de capa 4 (Transporte). Así pueden, entre otras cosas, realizar un filtrado en los puertos TCP o UDP e incluso realizar el análisis de datos de aplicación (capa 7).

2. Traductor de direcciones

En empresas grandes, distintas redes interconectadas pueden utilizar las mismas direcciones IP. Para que sea posible la comunicación entre nodos de los dos lados, hay que modificar las referencias del emisor del paquete, para que no haya conflicto y la transmisión sea fiable.

Los equipos de traducción de direcciones (NAT - *Network Address Translation*) se encargan de aportar esta funcionalidad. Permiten el cambio de una dirección IP por otra.

Hay tres tipos de traducción de dirección posibles:

- La traducción de puerto (PAT - *Port Address Translation*) funciona en una asignación dinámica de los puertos TCP o UDP, conservando la dirección IP original.
- La conversión dinámica de direcciones cambia la dirección IP instantáneamente, con relación a una externa disponible en una lista.
- La conversión estática de dirección, que también realiza un cambio de dirección IP, pero se mantiene una tabla que permite que se pueda sustituir una IP interna por la misma dirección IP externa.

Podemos observar que la conversión dinámica de direcciones permite disponer de menos direcciones externas que direcciones internas, lo que no ocurre en la conversión estática.

Una traducción de dirección IP también se puede realizar al salir de la red local. Esto permite ocultar la dirección privada interna. Este funcionamiento está previsto desde hace mucho tiempo y la RFC 1918 define rangos de direcciones utilizables en las redes privadas. Los tres espacios reservados son:

- 10.0.0.0, con una máscara de 8 bits (255.0.0.0).
- 172.16.0.0, con una máscara de 12 bits (de 172.16.255.254 a 172.31.255.254).
- 192.168.0.0, con una máscara de 16 bits (255.255.0.0).

Podemos observar que solo el primer rango de direcciones respeta el concepto de clase inicial, en este caso A.

Todas las demás direcciones son públicas y se pueden utilizar en Internet.

Así, por ejemplo, un equipo de la red local que realiza una solicitud a un sitio Web en Internet verá su dirección IP de emisor traducida en una dirección pública al salir de la LAN.

3. Cortafuegos

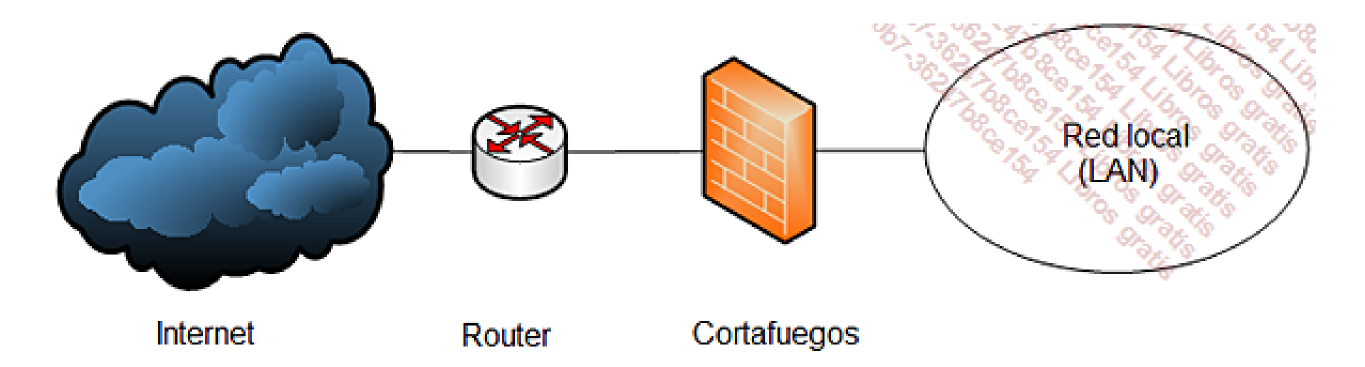
Un equipo de cortafuegos (*Firewall*) convierte las diferentes redes a las que se conecta en independientes. Al contrario que un router, no se conforma con transmitir la petición. Un cortafuegos segmenta los flujos asumiendo él mismo las peticiones. Para esto establece dos conexiones y puede realizar una acción de autenticación.


Esta segmentación también permite el cambio de la dirección del solicitante, como un mecanismo de traducción de direcciones.

La primera generación de estos equipos permitía distintos análisis en las cabeceras de los paquetes, de manera equivalente a los routers filtrantes. El cortafuegos de tabla de estado (*State full inspection*), más reciente, conserva en memoria una tabla de las conexiones establecidas. Así, las comunicaciones entre clientes, autorizadas después de la autenticación, pueden continuar sin problema.

La nueva generación de cortafuegos, llamada de aplicación, es capaz de analizar algunos cuerpos de paquetes, como los de los protocolos SMTP, HTTP... Este nivel de análisis permite atenuar las nuevas formas de ataque, que se aprovechan de los fallos de las aplicaciones estándar.

El cortafuegos de infraestructura suele ir acompañado de un cortafuegos personal, instalado en los equipos de trabajo. Así, los equipos se protegen de ataques que podrían proceder incluso de dentro de la red local.

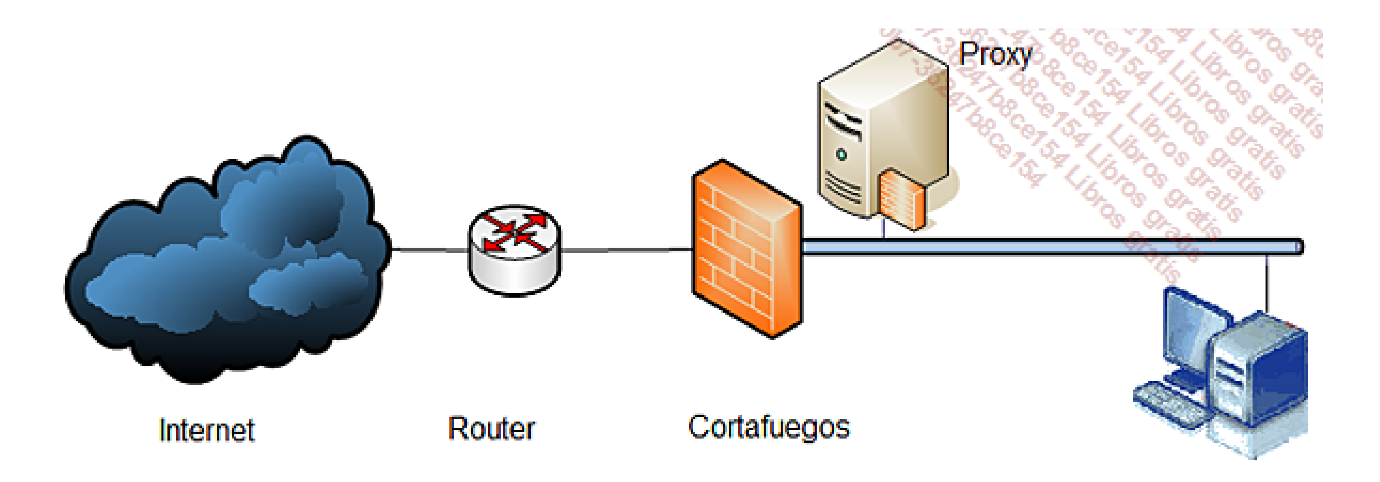


4. Proxy

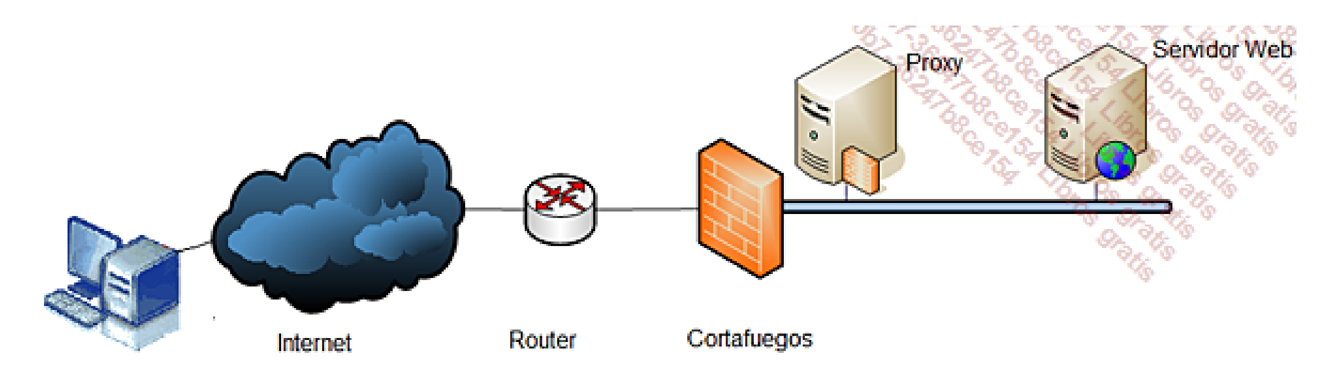
El servidor proxy se utiliza especialmente en el ámbito del tráfico *Hyper Text Transfer Protocol*(HTTP), o incluso con *File Transfer Protocol* (FTP), en la red LAN e Internet. Se puede considerar que es un complemento del cortafuegos.

Cuando intercepta una petición hacia el exterior, el proxy la redirige como si fuera suya y a continuación almacena los datos recibidos. Seguidamente, los envía al solicitante inicial. Proxy es interesante por dos razones. En primer lugar, camufla las direcciones IP internas, puesto que la petición no llega a Internet. Y luego permite filtrar para, por ejemplo, prohibir el acceso a algunos sitios Web.

Una tercera ventaja del proxy es su capacidad para administrar una memoria caché. Así pues, es posible volver a pedir un archivo o un sitio de Internet. A nivel Web, esta función es relativa. De hecho, un sitio dinámico cambia tan a menudo que se puede considerar que se carga en cada petición.



Un servidor proxy inverso (*reverse proxy*) intercepta una petición, por ejemplo de un sitio Web, procedente del exterior hacia un servidor interno. Esto permite evitar que estas peticiones lleguen a un servidor más vulnerable.

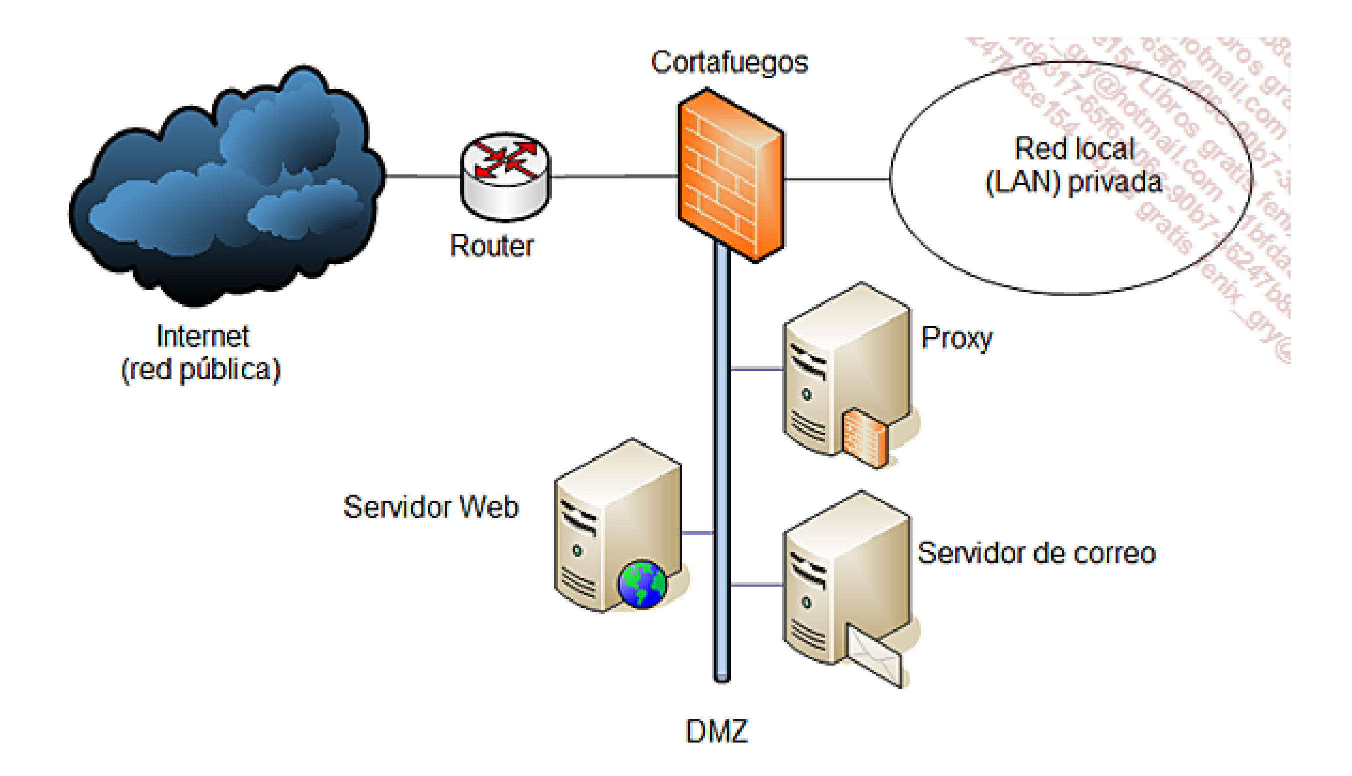


5. Zona desmilitarizada

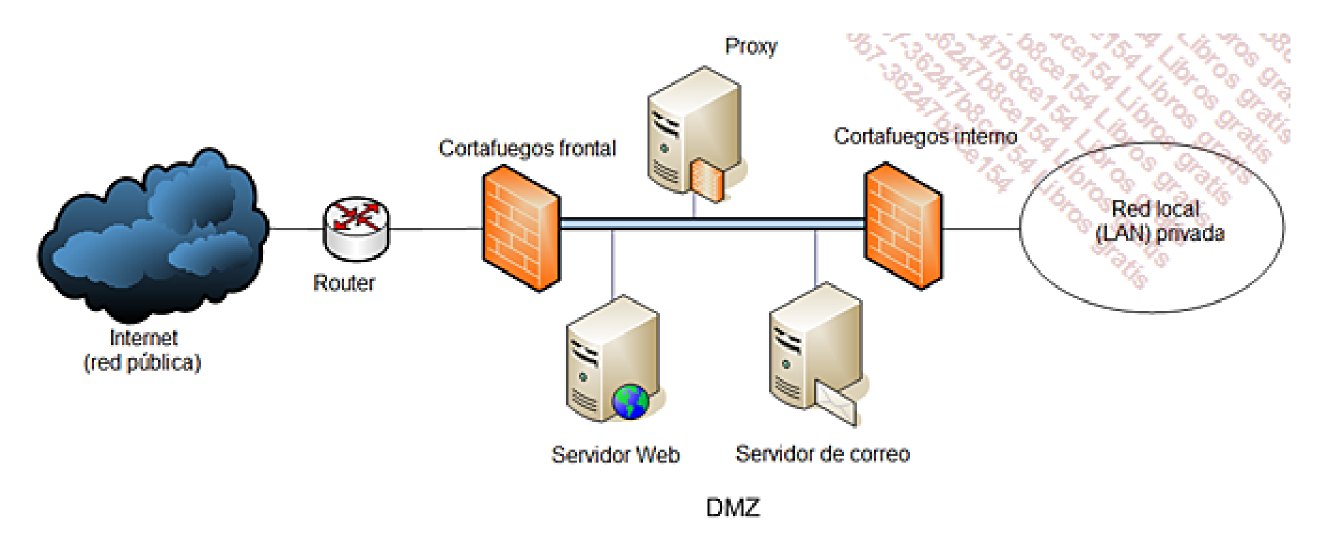
La interconexión entre la red pública Internet y la LAN a menudo utiliza una zona pública de*buffer* que está en la propia empresa. Esta zona se denomina «zona desmilitarizada» o*DeMilitarized Zone* (DMZ). Puede albergar diferentes servidores accesibles desde Internet, como:

- El servidor Proxy.
- El servidor Web que alberga el sitio de la empresa.
- El servidor de correo, encargado de seleccionar los mensajes.

La frontera de esta DMZ se concreta con al menos un cortafuegos. En infraestructuras de pequeño tamaño, suele ser un servidor para todo. En este caso, se le denomina trirresidente.



Las infraestructuras de mayor envergadura albergan una DMZ protegida por dos cortafuegos, uno por delante y otro por detrás. En este caso, se configuran de manera complementaria y generalmente son de marcas diferentes para que no presenten las mismas vulnerabilidades.



Método de enfoque

La resolución de un problema que afecta a la red requiere de rigor y metodología. Para ello es necesario tratar de dar respuesta a preguntas clave y respetar cierta progresión.

Por ejemplo, tratar de resolver el problema sin averiguar su causa generalmente conduce al fracaso.

En primer lugar, es preferible plantear cuestiones relativas a la aparición del incidente:

- ¿Ha funcionado antes?
- ¿Cuándo?
- ¿Qué modificación se ha realizado desde la última vez que funcionó?

Es importante centrarse en este momento únicamente en los hechos. Detenerse en las impresiones de los usuarios o en ideas preconcebidas no es eficaz.

Una metodología podría consistir en avanzar poco a poco, cumpliendo cada uno de los siguientes pasos:

1) Establecer los síntomas.

2) Identificar la amplitud del problema.

3) Definir lo que ha cambiado.

4) Elegir la causa más probable.

5) Implementar una solución.

6) Probar la solución.

7) Reconocer los efectos probables de la solución.

8) Documentar la solución.

Ejemplos de diagnóstico en capas bajas

Siempre hay que comprobar que los cables no estén expuestos a fuentes eléctricas o electromagnéticas que puedan crear interferencias. Por ejemplo, un cable de red que pasa por un canal compartido con cables eléctricos puede no funcionar bien. Del mismo modo, un cable que pasa muy cerca de un neón puede sufrir interferencias electromagnéticas (tubos fluorescentes). También puede haber un problema si el cableado pasa cerca de motores, por ejemplo, el de un ascensor. En estos casos, se puede utilizar cable blindado (STP) o incluso proteger el paso del cable cubriéndolo con una envoltura metálica.

Existen diferentes dispositivos que permiten probar el cableado de red.

1. Dispositivos

a. El téster de cables

Permite asegurarse del buen funcionamiento de un cable: ausencia de corte, medición de la atenuación, de la resistencia o de otras características. También proporciona información detallada de las propiedades mecánicas y eléctricas de un cable. Cuanto más largo sea el soporte físico utilizado, mayor será el riesgo de fallos. Por ejemplo, utilizar un cable de par trenzado de 150 metros aumenta considerablemente este riesgo.

Hoy en día hay tésters muy avanzados que permiten obtener información sobre las colisiones y otros elementos importantes vinculados a la disminución del rendimiento de la red.



Estos tésters (ohmímetros) permiten garantizar que la impedancia de los distintos componentes es la correcta. Por ejemplo, un valor infinito entre los dos extremos de un cable de par trenzado indica que el cable está partido.

b. El reflectómetro

El reflectómetro permite medir la distancia que hay desde este dispositivo hasta un corte de la red. Es posible seleccionar el tipo de cableado utilizado: coaxial o fibra. La señal rebota cuando el cable se ha cortado, de manera que resulta fácil determinar el tiempo de ida y vuelta para deducir la distancia hasta el corte.

Para garantizar un buen funcionamiento del reflectómetro, es necesario conectarlo a un extremo

de un segmento. Hay que apagar los posibles repetidores y puentes de red local para no interferir en las pruebas. En la mayoría de los casos, se aconseja detener completamente el funcionamiento de la red, a menos que el modelo de reflectómetro pueda trabajar con la red en funcionamiento.

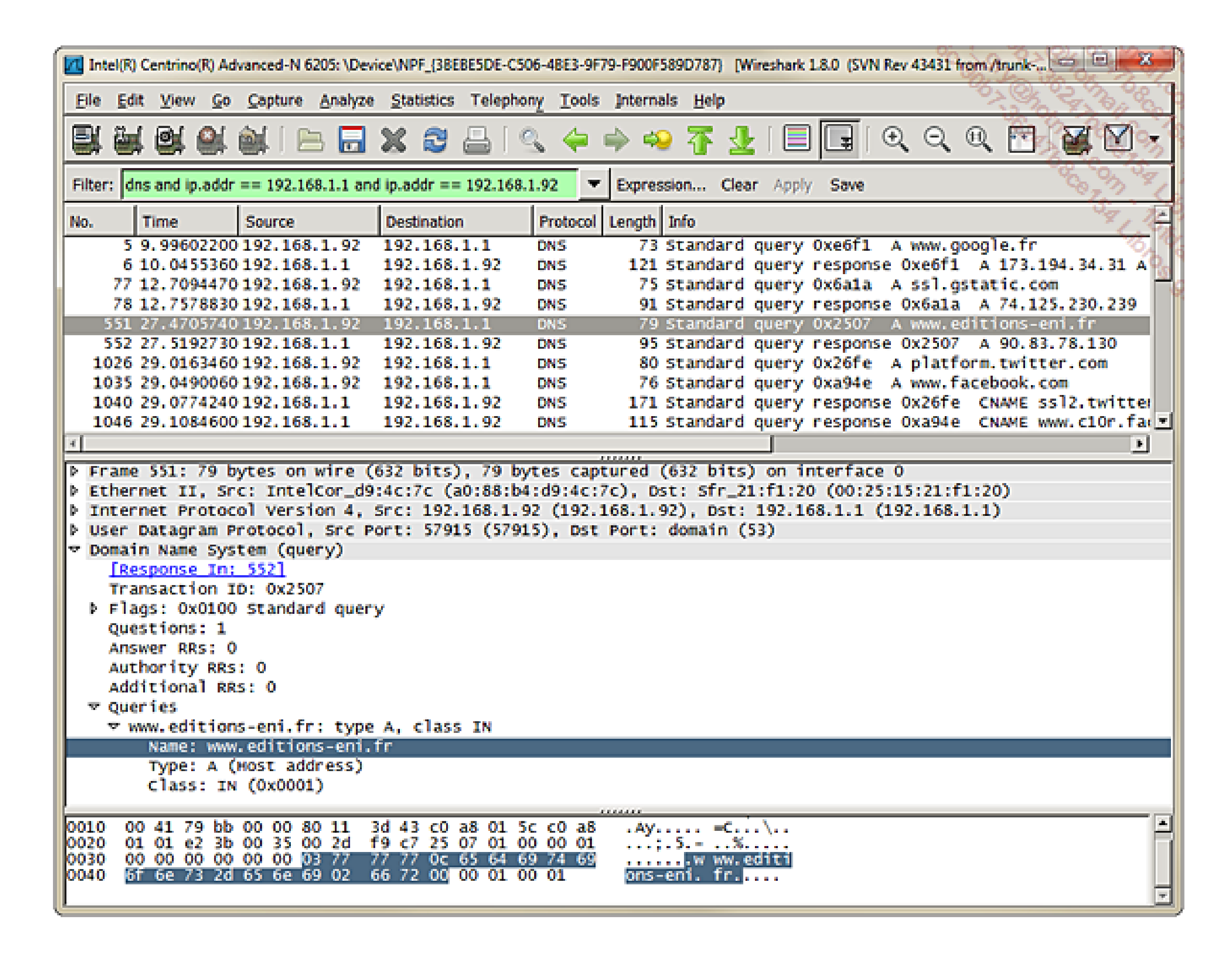


c. El voltímetro

También es posible utilizar un voltímetro para identificar un cable cortado o un cortocircuito. Este instrumento de medida permite aplicar una tensión a través de un cable para identificar el problema.

2. Análisis de tramas

Una herramienta de análisis de tramas (*sniffer*) permite efectuar un seguimiento de la actividad de la red y optimizar el rendimiento. Una herramienta detallada nos deja en condiciones de identificar de forma precisa el protocolo más utilizado a través de la red, el ordenador que intercambia más información o el protocolo que efectúa más difusiones. Esta herramienta no tiene, en cambio, la función de determinar si un cable se ha cortado o se ha cortocircuitado.



También se puede configurar para que controle, cuando sea conveniente, si un protocolo supera algún límite impuesto.

En general, dispone de una interfaz gráfica, que muestra los indicadores de los distintos dispositivos que se deben controlar.

3. Otros problemas con Ethernet

Como en el resto de las redes, los problemas pueden estar en las tarjetas de red (dispositivo, conector y configuración del software) o en los cables.

a. La unicidad de la dirección MAC

Cada tarjeta de red debe disponer, en una misma red lógica, de una dirección MAC distinta. Esto, en principio, no debe plantear problemas, puesto que en Ethernet, por definición, se utilizan direcciones IEEE preasignadas.

Sin embargo, y por desgracia, esto puede ocurrir, aunque muy raramente. Como hemos visto con anterioridad, los sistemas operativos permiten cambiar las direcciones MAC. Algunas tarjetas lo admiten directamente.

b. La configuración física de la tarjeta de red

Cuando no es posible lograr que la tarjeta funcione correctamente, lo primero que hay que hacer es comprobar que la configuración registrada en el dispositivo (en E2PROM) es la misma que la especificada en el entorno de utilización (sistema operativo).

No olvidemos que la mayoría de los sistemas operativos actuales a menudo son capaces de detectar la tarjeta de red, que no es lo mismo que establecer su configuración.

La segunda etapa consiste en comprobar que no existe ningún conflicto entre los distintos dispositivos configurados en el equipo. Los conflictos se producen muy raramente gracias a las detecciones automáticas de tipo Plug and Play y las resoluciones automáticas de problemas.

c. Parámetros de comunicación

El mal funcionamiento de algunas tarjetas produce paquetes cuya longitud es superior al máximo permitido (1538 bytes en Ethernet). Estos paquetes se pueden detectar en un equipo activo (por ejemplo, si se ilumina un indicador llamado Jabber) o mediante un analizador de tramas.

4. IPX y Ethernet

El problema más común que se puede encontrar en IPX es la incompatibilidad entre los tipos de tramas utilizados. Los distintos tipos de tramas que se pueden encontrar son los siguientes:

- Ethernet 802.2
- Ethernet 802.3
- Ethernet II
- o también Ethernet SNAP.

Estos tipos de tramas tienen diferencias pequeñas, pero son incompatibles. Por lo tanto, dos equipos que deseen comunicarse en una red Ethernet en IPX tienen que utilizar el mismo tipo de trama. Microsoft y Novell recomiendan utilizar el tipo de trama 802.2.

Este tipo de trama se instala automáticamente a partir de la versión 3.12 en los servidores Novell Netware.

Casi siempre el tipo de trama se detecta automáticamente y no se debe hacer nada. De hecho, el protocolo RIP IPX permite determinar la información incluida en el tipo de trama, necesaria para poder dialogar con el resto de la red. El problema llega cuando circulan simultáneamente diferentes tipos de trama en la red y los clientes están configurados para usar una por defecto.

5. Otros problemas con Token Ring

En el origen de los posibles problemas en un entorno Token Ring podemos encontrar diversos dispositivos: una tarjeta en conflicto con otros recursos, las direcciones asignadas, la velocidad especificada, los tipos de cables utilizados.

a. Conflicto de configuración

Lo primero que se debe comprobar es si la configuración utilizada por la tarjeta no entra en conflicto con otros dispositivos instalados en el equipo.

Observe las estadísticas elaboradas por la tarjeta para determinar si se han producido errores internos. Los errores internos son característicos de un mal funcionamiento del dispositivo e indican que se debe sustituir.

b. Configuración de la tarjeta Token Ring

El controlador del dispositivo proporcionado con la tarjeta debe permitir intervenir en cuatro de los parámetros esenciales para una tarjeta Token Ring: la velocidad del anillo, la dirección de la tarjeta, la memoria compartida utilizada, la liberación anticipada del testigo (solo en 16 Mbps).



Velocidad del anillo

Todas las tarjetas tienen que funcionar a la misma velocidad (4 o 16 Mbps).

Atención, una tarjeta Token Ring que funciona a una velocidad diferente a la del anillo generará una reconfiguración completa del anillo.

Dirección de la tarjeta

Las direcciones Token Ring se codifican en ROM, pero algunas tarjetas permiten su modificación. Como en Ethernet, dos tarjetas no pueden tener la misma dirección física. Podemos modificar la dirección.

Memoria compartida

Se debe indicar la dirección de memoria compartida utilizada por la tarjeta.

Liberación anticipada del testigo

En un anillo Token Ring a 16 Mbps, se puede liberar el testigo justo después de emitir la trama de datos. Esta funcionalidad similar a FDDI permite aumentar la velocidad real del anillo.

c. Conexión con los equipos

Hay que disponer de la documentación del cableado (arquitectura física y lógica) y de los equipos (modo de empleo, contraseña, configuraciones).

6. Otros problemas con FDDI

Los problemas que podemos encontrar con FDDI en general están vinculados a los conectores, al cableado y a los retrasos en la comunicación.

La suciedad o el polvo pueden provocar un mal funcionamiento en el intercambio de datos a través de la fibra. Se puede limpiar con un trapo y un poco de alcohol.

Pueden surgir otros problemas si un conector está defectuoso o si se ha cortado un cable.

La utilización de un buen tipo de fibra es indispensable. La fibra multimodo se puede emplear en segmentos que lleguen hasta dos kilómetros. Para distancias más largas, se recomienda usar fibra monomodo. Según el tipo de fibra utilizado, se pueden obtener velocidades más o menos elevadas. Así, con una fibra cuyo núcleo es de plástico, las distancias máximas son de 50 metros. Con un núcleo de vidrio, las distancias son considerablemente más grandes.

Un corte se puede detectar utilizando un reflectómetro óptico (¡muy caro!).

Utilización de herramientas TCP/IP adaptadas

1. Principios

El conjunto de protocolos TCP/IP proporciona numerosas herramientas que permiten comprobar el buen funcionamiento de la red o de un mecanismo específico: resolución de nombres, acceso a un ordenador...

Es importante conocer estas herramientas y familiarizarse con ellas.

2. Ejemplo de utilización de las herramientas

a. arp

El protocolo ARP mantiene localmente en el ordenador una tabla de correspondencias entre las direcciones IP (lógicas) y MAC (física). El comando «arp» permite editar esta tabla, que se encuentra en la memoria RAM.

Cuando no se puede alcanzar un destinatario a través de la red, es importante ver la máscara ARP del ordenador remoto para saber si dispone de la dirección MAC de la puerta de enlace predeterminada. En este caso, esto puede querer decir que la ida funciona, pero la vuelta no. Efectivamente, a la llegada, el router, que dispone de una interfaz en la misma red de nivel 2 que el destinatario, generará una petición ARP para obtener la dirección MAC de este. El destinatario recibirá la petición ARP y aprovechará para poner en su máscara la dirección MAC del ordenador que origina la petición ARP (el router), para anticipar la vuelta.

ARP también se puede utilizar para identificar un conflicto de dirección IP y comprobar la dirección MAC del destinatario en la misma red de nivel 2.

Podemos utilizar la herramienta ARP para añadir una entrada estática (mapeo de una dirección IP con una dirección MAC) para llegar a un dispositivo de red que no dispone de dirección IP (impresora) cuya dirección MAC conocemos. Para ello, efectuaremos una reserva ARP con la opción s.

En Unix/Linux es posible crear un archivo que contenga el mapeo entre las direcciones MAC y las direcciones IP (/etc/ethers) con el fin de minimizar el tráfico vinculado a las numerosas difusiones ARP. Junto con eso, y para añadir seguridad, ARP se puede desactivar en cada equipo de modo que nadie responda a una petición ARP solicitada por un ordenador desconocido cuya dirección MAC no esté referenciada en las tablas.

A continuación, se puede ver una máscara ARP de un ordenador Windows que dispone de cuatro tarjetas de red.

Observe que cada red de nivel 2 dispone de su propia máscara ARP.

```
C:\>arp -a
Interfaz: 172.16.0.100 --- 0x2
  Dirección IP          Dirección física      Tipo
  172.16.0.200          00-50-da-b8-22-9d     dinámico
  172.16.101.1          00-60-97-37-12-3b     dinámico
  172.16.103.1          00-50-da-d6-3e-e8     dinámico
  172.16.104.1          00-10-4b-b6-5b-27     dinámico
  172.16.205.1          00-50-04-ec-ae-4c     dinámico
  172.16.206.254        00-50-da-84-cb-62     dinámico
  172.16.208.1          00-50-da-36-33-91     dinámico
```

```
Interfaz: 172.20.0.100 --- 0x3
  Dirección IP          Dirección física      Tipo
  172.20.0.3            00-50-fc-4b-06-9c     dinámico
  172.20.0.57           00-60-97-c5-a8-ad     dinámico

Interfaz: 195.101.229.57 --- 0x1000005
  Dirección IP          Dirección física      Tipo
  195.101.229.60        00-20-6f-0d-75-c8     dinámico

Interfaz: 172.17.0.100 --- 0x1000006
  Dirección IP          Dirección física      Tipo
  172.17.0.3            00-50-fc-0b-39-f1     dinámico
  172.17.0.4            00-50-fc-54-0e-28     dinámico
  172.17.64.48          00-50-56-50-00-7f     dinámico
  172.17.71.1           00-50-fc-1f-7a-3a     dinámico
  172.17.207.89         00-50-fc-20-3a-39     dinámico

C:\>
```

A continuación se puede ver la máscara ARP de un ordenador Linux que tiene dos interfaces:

```
[root@linus /root]# arp -a
? (172.17.64.1) at 00:50:04:EC:AB:B8 [ether] on eth0
? (172.16.103.1) at 00:50:DA:D6:3E:E8 [ether] on eth1
? (172.16.102.1) at 00:50:FC:0B:39:F0 [ether] on eth1
? (172.16.208.1) at 00:50:DA:36:33:91 [ether] on eth1
? (172.17.1.146) at 00:10:5A:D8:3E:05 [ether] on eth0
? (172.17.0.218) at 00:50:FC:0B:3A:00 [ether] on eth0
? (172.16.1.253) at 00:04:00:A8:E0:B7 [ether] on eth1
router104 (172.16.104.1) at 00:10:4B:B6:5B:27 [ether] on eth1
jojo.eni.es (172.17.207.89) at 00:50:FC:20:3A:39 [ether] on eth0
? (172.17.3.6) at 00:50:FC:24:37:F3 [ether] on eth0
router205 (172.16.205.1) at 00:50:04:EC:AE:4C [ether] on eth1
? (172.16.206.254) at 00:50:DA:84:CB:62 [ether] on eth1
[root@linus /root]#
```

b. ping

El comando ping utiliza el protocolo ICMP. Permite comprobar si hay una buena conectividad de red, haciendo el envío de peticiones «echo request». La respuesta normal que se espera es «echo reply».

Es importante, cuando se realiza esta prueba hacia un equipo situado detrás de un router, conocer la puerta de enlace. El destinatario también debe conocer su puerta de enlace para enviar correctamente la respuesta. A menudo, el fallo de un «Ping» puede estar relacionado con una configuración defectuosa de la puerta de enlace o puede deberse a que las rutas están mal definidas en los routers.

Atención: cuando hay routers de filtrado o cortafuegos en la ruta, los paquetes ICMP echo request e ICMP echo reply pueden estar bloqueados. Para comprobar que no es así, debemos intentar conectarnos a un servicio que se ejecute en el ordenador remoto aunque el ping no funcione.

En este caso, el cortafuegos o el router de filtrado no dejará pasar más que algunos tipos de ICMP cuyo código conoce para impedir que los piratas obtengan demasiada información acerca de la asignación de direcciones de la red. Así, el ICMP echo request (ping de ida), corresponde al código 8 y al tipo 0, mientras que el ping de vuelta, ICMP echo reply, corresponde al código 0 y tipo 0.

La RFC 792 contiene los tipos y códigos ICMP, así como los mensajes asociados y su función.

El comando tracert/traceroute ayuda a establecer el diagnóstico en caso de que esta prueba no funcione.

Por ejemplo

Aquí tenemos un resultado desde un equipo de Windows:

```
C:\>ping 195.101.229.60
Haciendo ping a 195.101.229.60 con 32 bytes de datos:

Respuesta desde 195.101.229.60: bytes=32 tiempo<10 ms TTL=255
Respuesta desde 195.101.229.60: bytes=32 tiempo<10 ms TTL=255
Respuesta desde 195.101.229.60: bytes=32 tiempo<10 ms TTL=255
Respuesta desde 195.101.229.60: bytes=32 tiempo<10 ms TTL=255

Estadísticas de Ping para 195.101.229.60:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
C:\>
```

Este comando también se puede utilizar para obtener la lista de los equipos IP de una red de nivel 2, recurriendo a una difusión, como en Linux.

```
[root@linus /root]# ping 172.16.255.255
PING 172.16.255.255 (172.16.255.255): 56 data bytes
64 bytes from 172.16.0.2: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 172.16.1.253: icmp_seq=0 ttl=255 time=98.7 ms
(DUP!)
64 bytes from 172.16.0.2: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 172.16.1.253: icmp_seq=1 ttl=255 time=1.0 ms
(DUP!)
--- 172.16.255.255 ping statistics ---
2 packets transmitted, 2 packets received, +2 duplicates, 0%
packet loss
round-trip min/avg/max = 0.1/6.0/98.7 ms
```

c. tracert/traceroute

Este comando permite seguir la ruta completa del paquete IP hasta el destinatario y así identificar hasta dónde llega el paquete.

traceroute es una implementación Unix/Linux, mientras que los sistemas operativos Microsoft utilizan tracert.

Este comando intenta alcanzar la dirección IP o el nombre solicitados, limitándose a cruzar los routers de uno en uno hasta que el paquete alcanza el destinatario.

Haremos un tracert hasta un router de filtrado que bloquee este tipo de trama; de ahí el mensaje final que se obtiene.

```
D:\Windows\system32\cmd.exe

D:\Users\Juanki>tracert www.ediciones-eni.com

Traza a la dirección www.ediciones-eni.com [90.83.78.130]
sobre un máximo de 30 saltos:

  1     1 ms    <1 ms    <1 ms  livebox.home [192.168.1.1]
  2    25 ms    23 ms    22 ms  172.31.255.254
  3    23 ms    23 ms    22 ms  62.36.86.17
  4    23 ms    23 ms    23 ms  62.36.198.69
  5    24 ms    26 ms    24 ms  62.36.204.42
  6    25 ms    28 ms    26 ms  81.52.186.189
  7    23 ms    34 ms    28 ms  xe-2-1-1.barcr3.Barcelona.opentransit.net [193.2
51.242.29]
  8    41 ms    43 ms    43 ms  tengige2-10-0-10.pastr1.Paris.opentransit.net [1
93.251.242.41]
  9    44 ms    43 ms    43 ms  tengige0-1-0-4.auvtr1.Aubervilliers.opentransit.
net [193.251.243.29]
 10     *        *        *     Tiempo de espera agotado para esta solicitud.
 11     *        *        *     Tiempo de espera agotado para esta solicitud.
 12     *        *        *     Tiempo de espera agotado para esta solicitud.
 13     *        *        *     Tiempo de espera agotado para esta solicitud.
 14     *        *        *     Tiempo de espera agotado para esta solicitud.
 15     *        *        *     Tiempo de espera agotado para esta solicitud.
 16     *        *        *     Tiempo de espera agotado para esta solicitud.
 17     *        *        *     Tiempo de espera agotado para esta solicitud.
 18     *        *        *     Tiempo de espera agotado para esta solicitud.
 19     *        *        *     Tiempo de espera agotado para esta solicitud.
 20     *        *        *     Tiempo de espera agotado para esta solicitud.
 21     *        *        *     Tiempo de espera agotado para esta solicitud.
 22     *        *        *     Tiempo de espera agotado para esta solicitud.
 23     *        *        *     Tiempo de espera agotado para esta solicitud.
 24     *        *     ^C
D:\Users\Juanki>t
```

d. ipconfig/ifconfig

Este comando en sus distintas versiones permite indicar, identificar o renovar una configuración IP para un ordenador que dispone de una dirección IP fija o dinámica (cliente DHCP). Permite, entre otras cosas, conocer la dirección MAC de un equipo, así como algunas opciones definidas según el sistema operativo.

El comando en línea ipconfig se utiliza en Windows. En los sistemas Unix y Linux, el comando es ifconfig.

Estos comandos no funcionan de la misma manera. Únicamente ifconfig permite identificar una dirección IP, reactivar o desactivar una interfaz, mientras que las versiones de Microsoft solo permiten visualizar la configuración, o renovar o liberar una asignación en el caso de un cliente DHCP.

De este modo, ipconfig permite comprobar todos los parámetros efectivamente disponibles: IP, máscara, IP de la puerta de enlace, IP DNS 1, IP DNS 2, nombre de dominio, dirección MAC, nombre de servidor DHCP (cuando proceda),tipo de nodo NetBIOS...

Ifconfig proporciona menos detalles de las opciones TCP/IP, pero cubre mejor el funcionamiento de la red física: *Maximum Transfer Unit* (MTU), interfaz habilitada (U por UP) o deshabilitada (no se visualiza UP), dirección IP de difusión, situación del *multicast*, número de paquetes enviados, recibidos, IRQ y direcciones utilizadas por la tarjeta de red.

A continuación podemos ver la versión ampliada de un comando ejecutado en un servidor Windows, y después la versión sin `/all`.

```
C:\>ipconfig /all
Configuración IP de Windows 2000
        Nombre del host . . . . . . . . . : Ulysse
        Sufijo DNS principal . . .   . . . : eni-escuela.local
        Tipo de nodo. . . . . . . .  . . . : híbrido
        Enrutamiento habilitado . . . . . : Sí
        Proxy WINS habilitado . . . . . . : No
```

```
        Liste de búsqueda de sufijo DNS . : eni-escuela.local
                                            eni.local
Ethernet tarjeta 172.16. - eni publica :
        Sufijo de conexión específica DNS : eni.local
        Descripción . . . . . . . . . . . : Tarjeta Realtek RTL8139(A)
PCI Fast
```

```
Ethernet #3
        Dirección física. . . . . . . . . : 00-50-FC-0B-9A-80
        DHCP habilitado . . . . . . . . . : No
        Dirección IP. . . . . . . . . . . : 172.16.0.100
        Máscara de subred . . . . . . . . : 255.255.0.0
        Puerta de enlace predeterminada . :
        Servidores DNS. . . . . . . . . . :

Ethernet tarjeta 172.17. - eni privada :
        Sufijo de conexión específica DNS : eni.local
        Descripción . . . . . . . . . . . : Tarjeta Realtek RTL8139(A)
PCI Fast
Ethernet #2
        Dirección física. . . . . . . . . : 00-50-FC-1F-3C-6F
        DHCP habilitado . . . . . . . . . : No
        Dirección IP. . . . . . . . . . . : 172.17.0.100
        Máscara de subred . . . . . . . . : 255.255.0.0
        Puerta de enlace predeterminada . :
        Servidores DNS. . . . . . . . . . : 172.17.0.3
                                            172.17.0.4

C:\>ipconfig
Configuración IP de Windows 2000
Ethernet tarjeta 172.16. - eni pública :
        Sufijo de conexión específica DNS : eni.local
        Dirección IP. . . . . . . . . . . : 172.16.0.100
        Máscara de subred . . . . . . . . : 255.255.0.0
        Puerta de enlace predeterminada . :
Ethernet tarjeta 172.17. - eni privada :
        Sufijo de conexión específica DNS : eni.local
        Dirección IP. . . . . . . . . . . : 172.17.0.100
        Máscara de subred . . . . . . . . : 255.255.0.0
        Puerta de enlace predeterminada . :
```

El siguiente es un ejemplo obtenido en un sistema Linux que tiene dos tarjetas de red.

```
[root@linus /root]# ifconfig
eth0   Link encap:Ethernet  HWaddr 00:80:C8:D4:98:01
       inet addr:172.17.0.2  Bcast:172.17.255.255  Mask:255.255.0.0
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:16868111 errors:0 dropped:0 overruns:0 frame:0
       TX packets:22140084 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:100
       Interrupt:11 Base address:0x6600
eth1   Link encap:Ethernet  HWaddr 00:50:FC:24:D8:6E
       inet addr:172.16.0.2  Bcast:172.16.255.255  Mask:255.255.0.0
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:38581402 errors:0 dropped:0 overruns:0 frame:0
       TX packets:60438451 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:100
       Interrupt:9 Base address:0x6500
lo     Link encap:Local Loopback
       inet addr:127.0.0.1  Mask:255.0.0.0
       UP LOOPBACK RUNNING  MTU:3924  Metric:1
       RX packets:12903 errors:0 dropped:0 overruns:0 frame:0
       TX packets:12903 errors:0 dropped:0 overruns:0 carrier:0
```

```
      collisions:0 txqueuelen:0

[root@linus /root]#
```

e. netstat

Este comando permite visualizar, por una parte, los puertos abiertos de un ordenador y, por otra parte, la tabla de enrutamiento del ordenador local o incluso las estadísticas de funcionamiento de la red.

A continuación se puede ver el resultado en un ordenador Windows.

```
C:\>netstat -an
Conexiones activas
  Proto  Dirección local        Dirección remota       Estado
  TCP    0.0.0.0:23             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3911           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:4512           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:4610           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:12345          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1029         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1031         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1766         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3532         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3910         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3928         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:4563         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:4564         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:4565         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:4566         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:4608         0.0.0.0:0              LISTENING
  TCP    172.17.0.89:1337       0.0.0.0:0              LISTENING
  TCP    172.17.0.89:1619       0.0.0.0:0              LISTENING
  TCP    172.17.0.89:1878       0.0.0.0:0              LISTENING
  TCP    172.17.207.89:139      0.0.0.0:0              LISTENING
  TCP    172.17.207.89:2411     0.0.0.0:0              LISTENING
  TCP    172.17.207.89:2904     0.0.0.0:0              LISTENING
  TCP    172.17.207.89:2964     0.0.0.0:0              LISTENING
  TCP    172.17.207.89:3299     0.0.0.0:0              LISTENING
  TCP    172.17.207.89:3514     0.0.0.0:0              LISTENING
  TCP    172.17.207.89:3799     0.0.0.0:0              LISTENING
  TCP    172.17.207.89:3905     0.0.0.0:0              LISTENING
  TCP    172.17.207.89:3905     172.17.0.2:1a39        ESTABLISHED
  TCP    172.17.207.89:3911     172.17.0.100:34703     ESTABLISHED
  TCP    172.17.207.89:4610     172.17.0.100:3389      ESTABLISHED
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1030           *:*
  UDP    0.0.0.0:1033           *:*
  UDP    0.0.0.0:1054           *:*
  UDP    0.0.0.0:3912           *:*
  UDP    0.0.0.0:4611           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:2234         *:*
  UDP    127.0.0.1:3929         *:*
  UDP    172.17.207.89:123      *:*
  UDP    172.17.207.89:137      *:*
  UDP    172.17.207.89:138      *:*
  UDP    172.17.207.89:1900     *:*
```

Seguidamente se representa un extracto de la tabla de enrutamiento de un servidor Windows.

```
C:\>netstat -rn
Tabla de rutas
=========================================================================
Lista de interfaces
0x1 ........................... MS TCP Loopback interface
0x2 ...00 50 fc 0b 9a 80 ...... NDIS 5.0 driver
                                  (Microsoft's Packet Scheduler)
0x3 ...00 80 c8 ec 81 e5 ...... VIA PCI 10/100Mb Fast Ethernet
Adapter (Microsoft's Packet Scheduler)
0x1000005 ...00 50 fc 0b af 96 ...... NDIS 5.0 driver
                                  (Microsoft's Packet Scheduler)

=========================================================================
Rutas activas:
Destino de red    Máscara de red    Puerta de acceso Interfaz   Métrica
      127.0.0.0         255.0.0.0       127.0.0.1     127.0.0.1        1
     172.16.0.0       255.255.0.0    172.16.0.100  172.16.0.100        1
   172.16.0.100   255.255.255.255       127.0.0.1     127.0.0.1        1
 172.16.255.255   255.255.255.255    172.16.0.100  172.16.0.100        1
     172.17.0.0       255.255.0.0    172.17.0.100  172.17.0.100        1
   172.17.0.100   255.255.255.255       127.0.0.1     127.0.0.1        1
  72.17.255.255   255.255.255.255    172.17.0.100  172.17.0.100        1
     172.20.0.0       255.255.0.0    172.20.0.100  172.20.0.100        1
   172.20.0.100   255.255.255.255       127.0.0.1     127.0.0.1        1
 172.20.255.255   255.255.255.255    172.20.0.100  172.20.0.100        1
    192.168.1.0     255.255.255.0    172.16.101.1  172.16.0.100        1
    192.168.2.0     255.255.255.0    172.16.102.1  172.16.0.100        1
    192.168.3.0     255.255.255.0    172.16.103.1  172.16.0.100        1
    192.168.4.0     255.255.255.0    172.16.104.1  172.16.0.100        1
    192.168.5.0     255.255.255.0    172.16.205.1  172.16.0.100        1
    192.168.6.0     255.255.255.0    172.16.206.1  172.16.0.100        1
    192.168.7.0     255.255.255.0    172.16.207.1  172.16.0.100        1
    192.168.8.0     255.255.255.0    172.16.208.1  172.16.0.100        1
   192.168.11.0     255.255.255.0    172.16.101.1  172.16.0.100        1
   192.168.12.0     255.255.255.0    172.16.102.1  172.16.0.100        1
   192.168.13.0     255.255.255.0    172.16.103.1  172.16.0.100        1
   192.168.14.0     255.255.255.0    172.16.104.1  172.16.0.100        1
   192.168.15.0     255.255.255.0    172.16.205.1  172.16.0.100        1
   192.168.16.0     255.255.255.0    172.16.206.1  172.16.0.100        1
   192.168.17.0     255.255.255.0    172.16.207.1  172.16.0.100        1
   192.168.18.0     255.255.255.0    172.16.208.1  172.16.0.100        1
      224.0.0.0         224.0.0.0    172.16.0.100  172.16.0.100        1
      224.0.0.0         224.0.0.0    172.17.0.100  172.17.0.100        1
      224.0.0.0         224.0.0.0    172.20.0.100  172.20.0.100        1
255.255.255.255   255.255.255.255    172.16.0.100  172.16.0.100        1

Puerta de enlace predeterminada:
=========================================================================
Rutas persistentes:
Dirección de red    Máscara de red      Dirección puerta enl. Métrica
    192.168.11.0    255.255.255.0       172.16.101.1         1
     192.168.1.0    255.255.255.0       172.16.101.1         1
     192.168.2.0    255.255.255.0       172.16.102.1         1
    192.168.12.0    255.255.255.0       172.16.102.1         1
     192.168.3.0    255.255.255.0       172.16.103.1         1
    192.168.13.0    255.255.255.0       172.16.103.1         1
     192.168.4.0    255.255.255.0       172.16.104.1         1
    192.168.14.0    255.255.255.0       172.16.104.1         1
     192.168.5.0    255.255.255.0       172.16.205.1         1
    192.168.15.0    255.255.255.0       172.16.205.1         1
     192.168.6.0    255.255.255.0       172.16.206.1         1
    192.168.16.0    255.255.255.0       172.16.206.1         1
```

```
     192.168.7.0     255.255.255.0       172.16.207.1          1
    192.168.17.0     255.255.255.0       172.16.207.1          1
     192.168.8.0     255.255.255.0       172.16.208.1          1
    192.168.18.0     255.255.255.0       172.16.208.1          1
   192.168.206.0     255.255.255.0     172.16.206.254          1
```

f. nbtstat

Esta herramienta NBT permite, en un sistema operativo Microsoft, visualizar las aplicaciones NetBIOS arrancadas o ver la caché local de los nombres NetBIOS resueltos en direcciones IP.

Es fácil comprobar, con la ayuda de este comando, que el ordenador inicializó sus servicios NetBIOS correctamente.

A continuación indicamos las aplicaciones NetBIOS inicializadas en un ordenador Windows Server multiservicios (que además dispone de varias interfaces):

```
C:\>nbtstat -n

172.16. - eni pública:
Dirección IP: [172.16.0.100] ID de ámbito: []

             Tabla de nombres locales NetBIOS
    Nombre               Tipo        Estado
    -----------------------------------------
    ULYSSE         <00>  único       Registrado
    ENI-ESCUELA          Grupo       Registrado
    ULYSSE               único       Registrado
    ULYSSE         <20>  único       Registrado
    ENI-ESCUELA    <1E>  Grupo       Registrado
    INet~Services        Grupo       Registrado
    IS~ULYSSE......<00>  único       Registrado

172.20. - DMZ privada:
Dirección IP: [172.20.0.100] ID de ámbito: []
   No hay nombres en la caché

172.17. - eni privada:
Dirección IP: [172.17.0.100] ID de ámbito : []

             Tabla de nombres locales NetBIOS
    Nombre               Tipo        Estado
    -----------------------------------------
    ULYSSE         <00>  único       Registrado
    ENI-ESCUELA    <00>  Grupo       Registrado
    ULYSSE         <03>  único       Registrado
    ULYSSE         <20>  único       Registrado
    ENI-ESCUELA    <1E>  Grupo       Registrado
    INet~Services  <1C>  Grupo       Registrado
    IS~ULYSSE......<00>  único       Registrado

C:\>
```

También podremos (con la opción -n) comprobar si efectivamente un servidor es controlador de dominio (Nombre de dominio). Observe que esta operación se puede realizar en remoto con -a o -A.

Este comando también es interesante para identificar los nombres NetBIOS de ordenadores duplicados en la red.

En este ejemplo, el comando nbtstat -c permite ver la lista de nombres NetBIOS que se han resuelto en direcciones IP:

```
C:\>nbtstat -c
```

```
172.16. - eni pública:
Dirección IP: [172.16.0.100] ID de ámbito: []

                  Tabla de nombres de caché remota NetBIOS

    Nombre               Tipo     Dirección de host    Duración [sec]
    -----------------------------------------------------------------
    DEMETER        <20>  único        172.16.0.200              422

172.20. - DMZ privada:
Dirección IP: [172.20.0.100] ID de ámbito: []

    No hay nombres en la caché
172.17. - eni privada:
Dirección IP: [172.17.0.100] ID de ámbito: []

                  Tabla de nombres de caché remota NetBIOS

    Nombre               Tipo     Dirección de host    Duración [sec]
    -----------------------------------------------------------------
    CD1            <20>  único          172.17.0.4              440
    HERMES         <20>  único          172.17.0.3              340

C:\>
```

g. nslookup

nslookup permite comprobar el buen funcionamiento de las resoluciones de nombres DNS.

Una vez ejecutada la herramienta, se pueden hacer diversas consultas, tal y como muestra la pantalla que se reproduce a continuación en un sistema Windows.

```
D:\Windows\system32\cmd.exe - nslookup -

D:\Users\Juanki>nslookup -
Servidor predeterminado:  livebox.home
Address:  192.168.1.1

> www.google.es
Servidor:  livebox.home
Address:  192.168.1.1

Respuesta no autoritativa:
Nombre:  www.google.es
Addresses:  173.194.45.24
          173.194.45.31
          173.194.45.23

> set type=CNAME
> www.google.es
Servidor:  livebox.home
Address:  192.168.1.1

google.es
        primary name server = ns2.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 1511898
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
> set type=NS
> google.es
Servidor:  livebox.home
Address:  192.168.1.1

Respuesta no autoritativa:
google.es       nameserver = ns4.google.com
google.es       nameserver = ns1.google.com
google.es       nameserver = ns2.google.com
google.es       nameserver = ns3.google.com

ns1.google.com  internet address = 216.239.32.10
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
ns4.google.com  internet address = 216.239.38.10
>
```

Por ejemplo, para comprobar que el equipo es capaz de resolver nombres DNS (para llegar al servidor DNS adecuado), basta con indicar el nombre del dominio, incluso de un equipo. Si el servidor DNS de referencia no puede dar la respuesta directamente, indicará la dirección IP del servidor que autoriza. También es posible consultar a un DNS para saber cuál es o cuáles son los servidores de correo registrados (Tipo = MX).

Esta herramienta es muy avanzada y su dominio requiere un poco más de conocimiento que las anteriores.

La pila de protocolos TCP/IP de los sistemas operativos Windows utiliza una caché DNS, que permite sistemáticamente consultar al servidor de nombres. El contenido de esta caché se puede visualizar con el comando «ipconfig /displaydns». Es muy útil en las tareas diarias, pero puede resultar negativa si hay algún error. De hecho, si no se resuelve un nombre, la información permanece unos instantes en la caché, aunque se haya corregido el error. En este caso es necesario reinicializar la información con el comando «ipconfig /flushdns».

Como se ve a continuación, este comando funciona en modo interactivo o en modo de línea de comandos. En este último caso, cualquier operación se introduce en una sola línea.

```
C:\>nslookup
Servidor predeterminado: hermes.eni-escuela.local
Dirección:  172.17.0.3

> ls eni-escuela.local
[hermes.eni-escuela.local]
 eni-escuela.local.           A      172.20.0.3
```

```
 eni-escuela.local.           A      172.17.0.3
 eni-escuela.local.           A      172.17.0.4
 eni-escuela.local.           NS     server = cd1.eni-escuela.local
 eni-escuela.local.           NS     server = hermes.eni-escuela.local
 2000test                     A      172.17.71.4
 gc._msdcs                    A      172.17.0.4
 gc._msdcs                    A      172.17.0.3
 gc._msdcs                    A      172.20.0.3
 ADW2KSRV                     A      172.17.35.31
 adxppro                      A      172.17.35.35
 bmartin                      A      172.17.1.159
 brunom                       A      172.17.159.1
 cd1                          A      172.17.0.4
 demeter                      A      172.17.0.200
 dyonisos                     A      172.17.0.89
 eliane2                      A      172.17.202.1
 erickpro                     A      172.17.71.3
 ericxp                       A      172.17.71.1
 gilles                       A      172.17.201.10
 gilles2                      A      172.17.201.3
 hermes                       A      172.20.0.3
 hermes                       A      172.17.0.3
 jerome                       A      172.17.1.146
 linus                        A      172.17.0.2
 lotus                        NS     server = ptmail01.lotus.
eni-escuela.local
 ptmail01.lotus               A      172.17.35.31
 ptmail01                     A      172.17.35.31
 sandrine2                    A      172.17.202.2
 sophie3                      A      172.17.1.18
 srv-h                        A      172.17.64.12
 stephane                     A      172.17.104.205
 ulysse                       A      172.17.0.100
 vero-xp                      A      172.17.3.6
 xp-pro-vm-eric               A      172.17.71.100
>

C:\>nslookup www.microsoft.com
Servidor :  hermes.eni-escuela.local
Dirección:  172.17.0.3

Respuesta no autoritativa:
Nombre :    www.microsoft.akadns.net
Dirección:  207.46.134.155
Aliases  :  www.microsoft.com

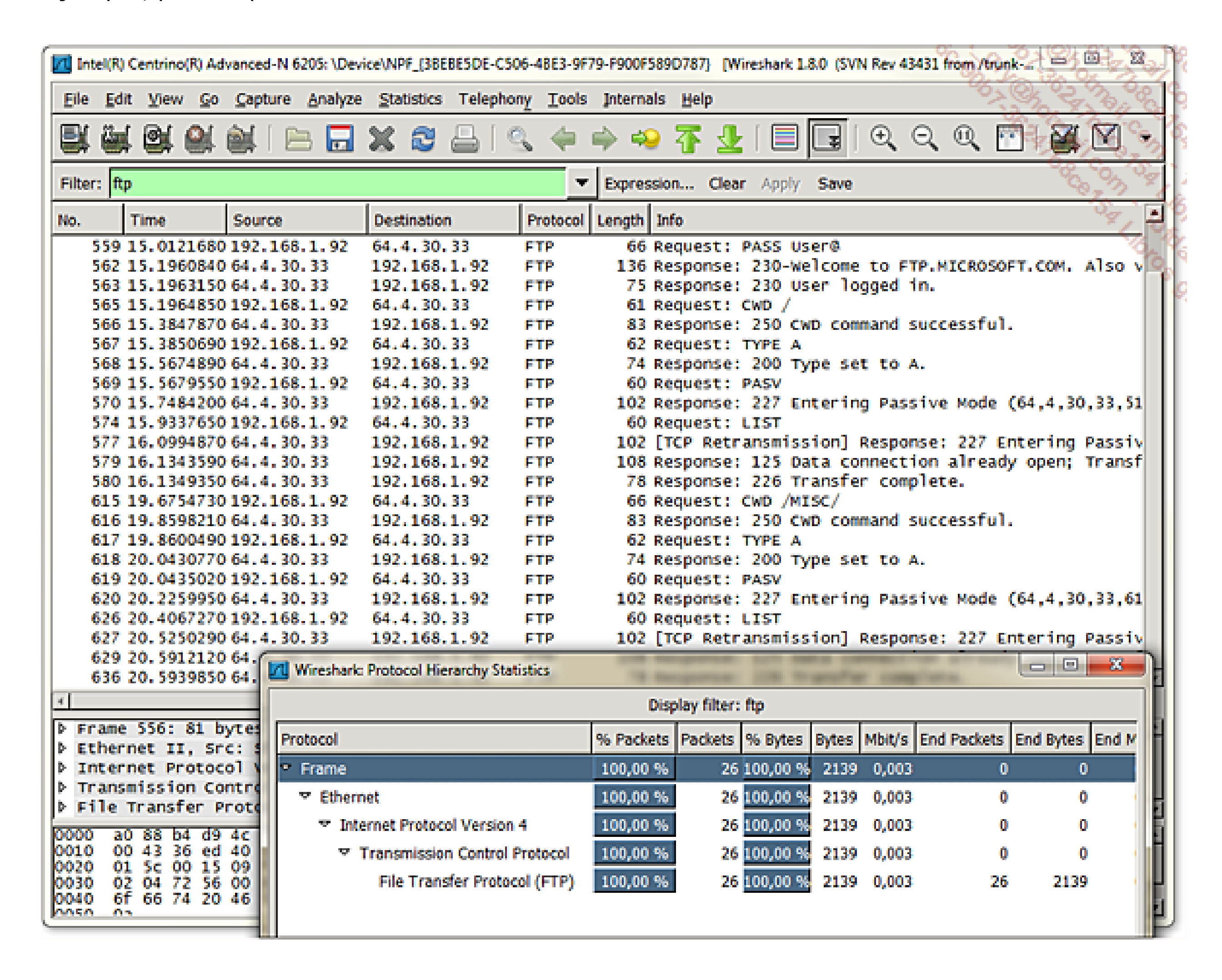
C:\>
```

Herramientas de análisis de capas altas

1. Análisis de peticiones de aplicaciones

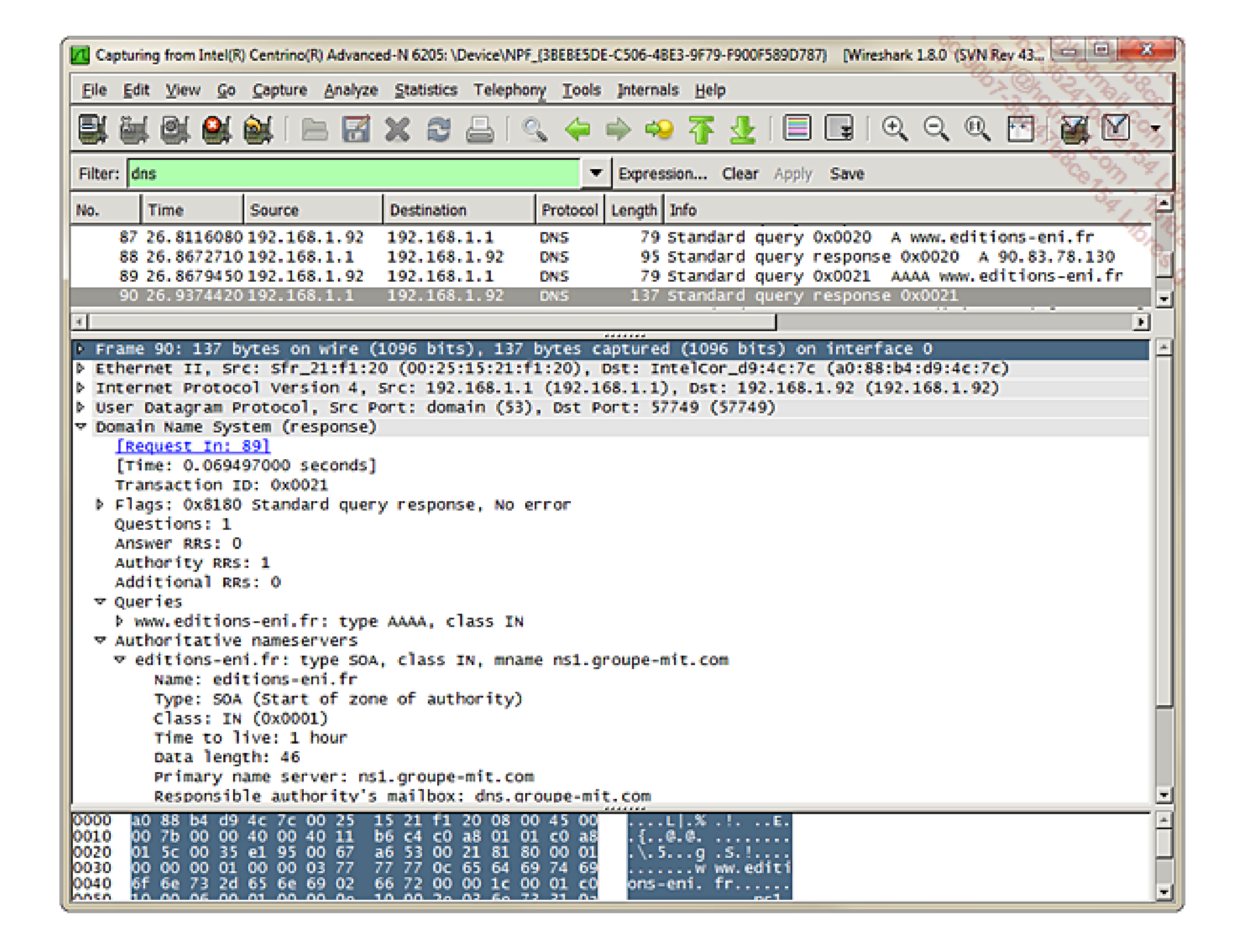
Para el análisis de aplicaciones, la herramienta más interesante es un analizador de tramas como Wireshark.

Por ejemplo, para capturar tramas FTP:



Análisis de tramas FTP

O incluso para analizar peticiones DNS:



Ejemplo de análisis de una respuesta DNS

2. Análisis de peticiones web

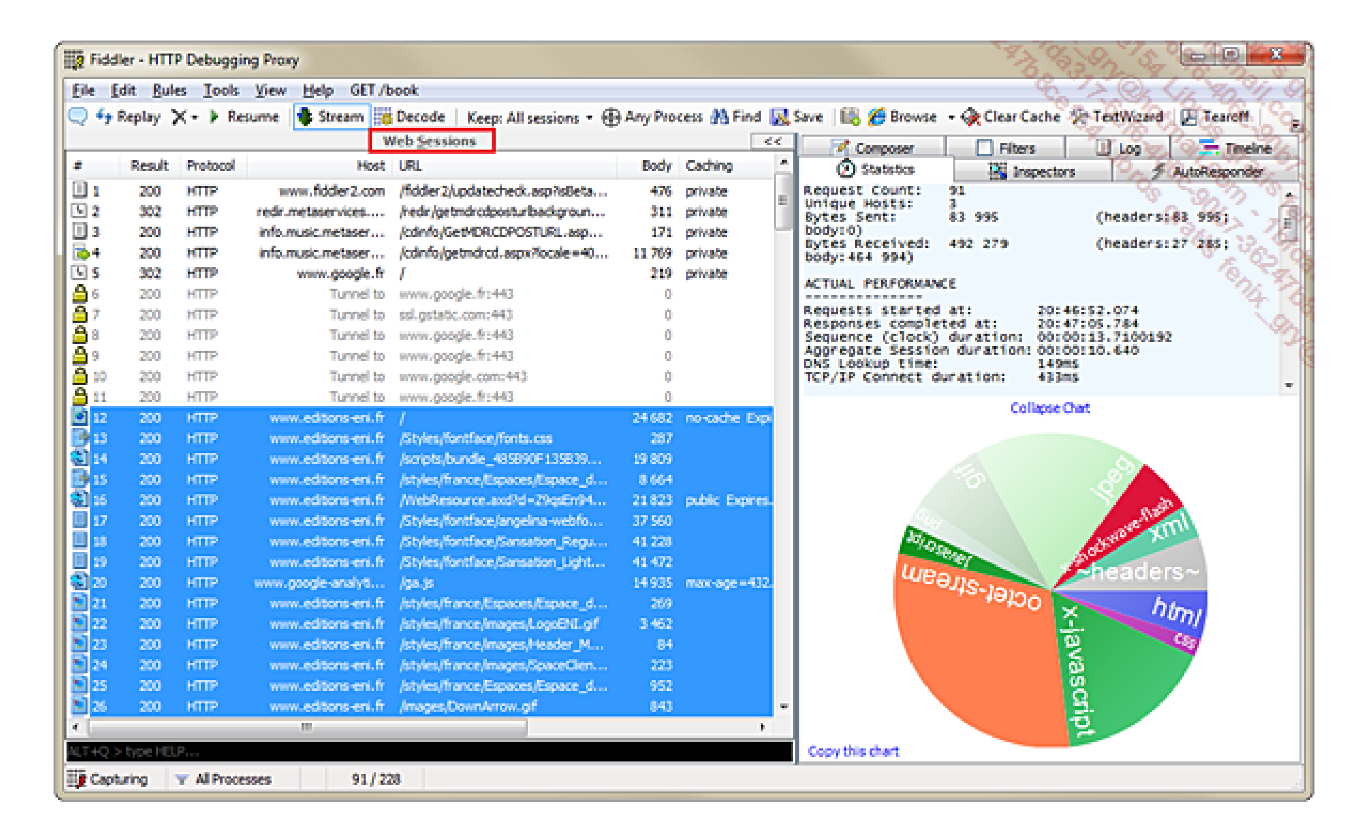
Por otra parte, existe una herramienta más específica para entornos web.

Por ejemplo, **Fiddler**, que significa literalmente «violinista», permite analizar las tramas entre un navegador y un servidor web.

Se trata de un depurador HTTP que actúa como proxy. Funciona automáticamente con Internet Explorer, pero puede funcionar igualmente, si se configura, con otros navegadores.

Utiliza la dirección IP de bucle local en IPv4 (127.0.0.1) en el puerto 8888.

Cada petición web que ha ido a través del proxy aparece como una línea en el apartado *Web Sessions*.



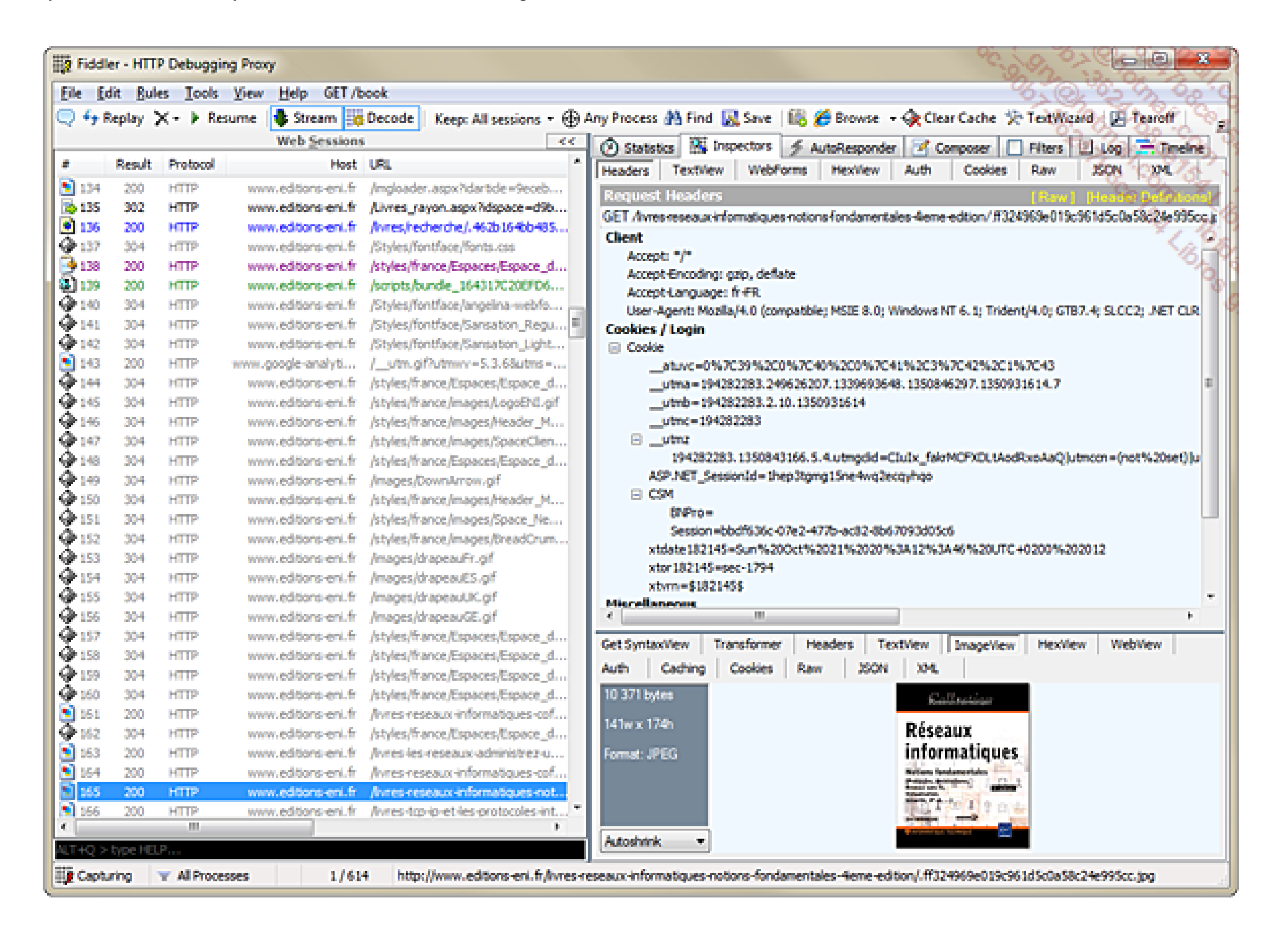
Análisis de tramas con Fiddler2

Es posible utilizar javascript para analizar o modificar peticiones HTTP.

- Se trata en particular de una de las curiosas herramientas disponibles para analizar cada petición AJAX.

Descomposición de la visualización de un sitio web

Permite reproducir una secuencia completa de tramas capturadas, crear puntos de parada para realizar ejecuciones paso a paso, obtener estadísticas instantáneas o efectuar búsquedas completas de una palabra clave en un flujo HTTP.



Visualización de las cookies, búsqueda de imágenes

- Fiddler está disponible gratuitamente en la URL http://www.fiddler2.com/. Solo existe versión para Windows y necesita el framework .NET.

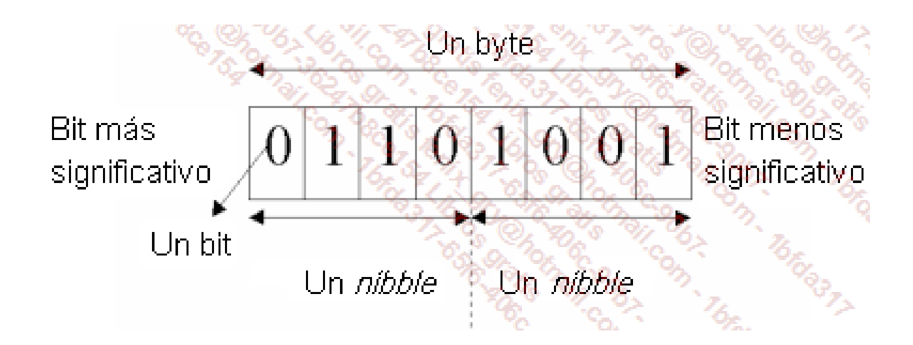
- Hay vídeos en inglés que muestran algunas de las posibilidades que ofrece Fiddler:http://fiddler2.com/support

Conversión de decimal (base 10) a binario (base 2)

1. Vocabulario utilizado

¡En informática, todo es digital! La información se representa en forma de 0 o de 1, de verdadero o de falso, de condensador cargado o no.

Se trata de una representación de dos estados.



La información se agrupa en bytes; un byte son 8 bits.

Un bit representa dos estados, o dos posibilidades; dos bits permiten 4 (2 x 2).

Así, un byte permite representar 256 combinaciones posibles.

Según los sistemas utilizados, podremos codificar información distinta entre 0 y 255 o, con signo, entre -127 y +128 (con el 0 corresponde a 256 posibilidades).

2. Conversión a partir de base 10

Imaginemos un valor que deseamos convertir en binario, por ejemplo 2003.

En primer lugar, escribimos la lista de las potencias de 2 comenzando por 1, lo que viene a ser lo mismo que efectuar una sucesión de multiplicaciones por 2, comenzando por el valor 1 hasta obtener un número superior a 2003.

Obtenemos:

1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048

Observe que, entre los números encontrados, la suma de algunos de ellos permite obtenerexactamente 2003.

Dicho de otra forma, cogiendo solo una vez algunos de los números encontrados (las potencias de 2) inferiores a 2003, podemos obtener 2003.

Un consejo: hay que empezar siempre por el más grande y seguir hacia el más pequeño.

Ahora solo nos queda saber aquellos que utilizaremos y, cada vez, restar para ver qué valor es el que nos falta por descomponer.

De este modo, para 2003 empezamos con 1024 y nos faltan 979 (2003-1024).

979 se descompone en 512 + 467

467 = 256 + 211

211 = 128 + 83

83 = 64 + 19

19 = 16 + 3

3 = 2 + 1

Entonces, 2003 = 1024 + 512 + 256 +128 + 64 + 16 + 2 + 1.

Escribamos nuestra lista en sentido inverso, indicando si hemos utilizado o no este valor para encontrar la suma buscada:

2048	1024	512	256	128	64	32	16	8	4	2	1
NO	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	NO	NO	SÍ	SÍ
2048	1024	512	256	128	64	*32*	16	*8*	*4*	2	1

¡Colocamos un '0' cuando no lo utilizamos y un '1' si lo utilizamos.

Finalmente obtenemos 011111010011.

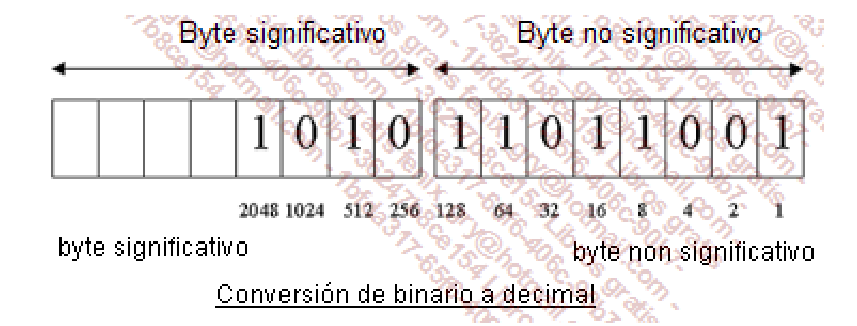
¡Y ya está!

Conversión de binario (base 2) a decimal (base 10)

1. Conversión desde un binario

Supongamos un número escrito en binario, por ejemplo 101011011001.

Será necesario colocar en casillas, empezando por la derecha, los valores 1 y 0, numerando las casillas de derecha a izquierda con potencias de 2.



Simplemente basta con añadir los valores que corresponden a las casillas que contienen un 1.

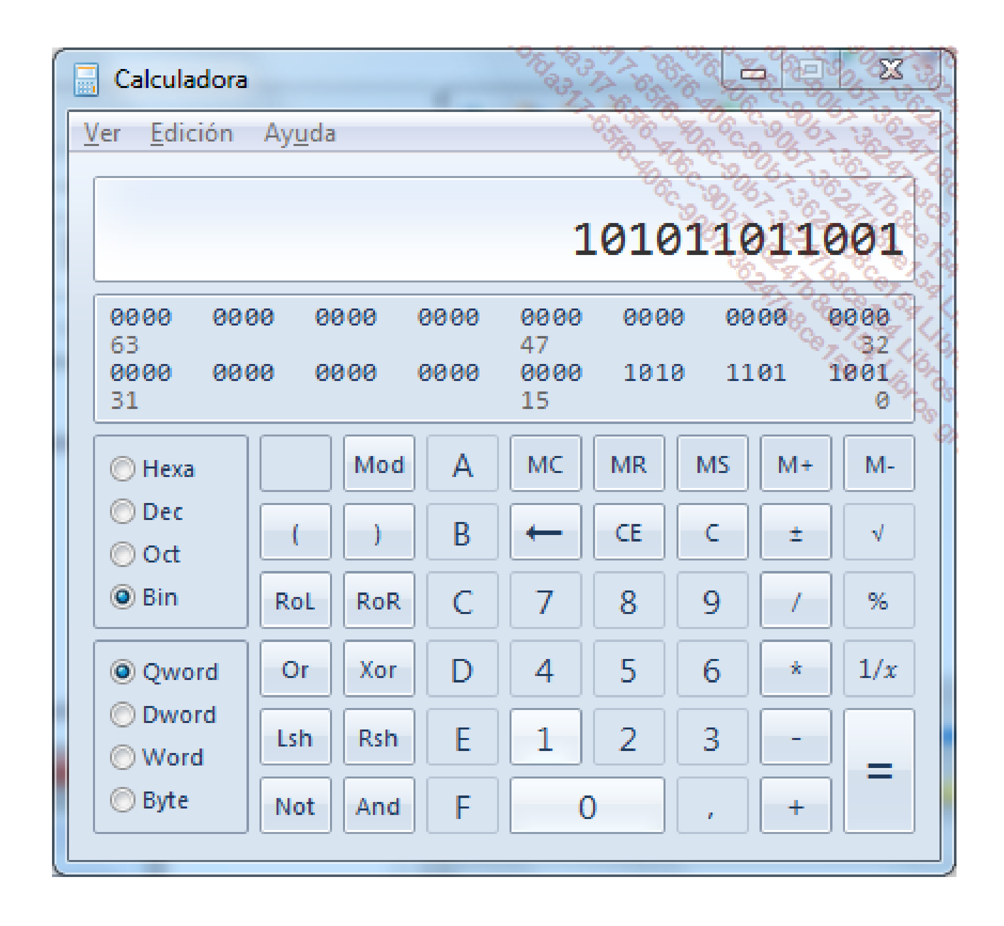
En este caso, obtenemos:

2048 + 512 + 128 + 64 + 16 + 8 + 1 = 2777

Es mucho más sencillo, ¿no?

En cualquier caso, tenemos la calculadora de Windows en modo Programador.

Una vez seleccionada la opción binaria (bin), solo tiene que elegir la sucesión de '0' y '1':



Solo tiene que seleccionar **Dec** para obtener la conversión deseada.

Conversión de hexadecimal (base 16) a decimal (base 10)

Con las direcciones IPv6, el formato hexadecimal vuelve con nosotros. Aunque raramente se «cortan» los bytes en la descomposición en subredes, puede ser interesante utilizar las conversiones.

La calculadora en modo programador le puede ayudar en todos los casos.

Un método sencillo para comprender el formato hexadecimal es acercarse a la escritura binaria del byte.

Hexadecimal significa literalmente «6» (hexa) y «10» (decimal).

Un símbolo hexadecimal se representa por cifras (0 a 9) y letras (A a F).

Así, para contar de 0 a 15, se enumera 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F.

Donde **A** vale **10**, **B** vale **11** y así hasta **F**, que vale **15**.

Cada vez que se añade un símbolo '0' a la derecha de un número, se multiplicará por la base (16).

Así, **A** significa **10** en base 10, **A0** corresponde a **160** y **A00** a **2560** (10 x 16 x 16).

Pongamos como ejemplo para convertir AC73 en decimal.

A corresponde a **10**, **C** a **12**.

3 está situado como la unidad (16 elevado a 0 = 16^0= 1).

7 se debe multiplicar por la base (16 elevado a 1 = 16).

C se debe multiplicar dos veces por la base (16^2).

A se multiplicará tres veces por la base (16^3).

Se obtiene:

Peso	16 x 16 x 16	16 x 16	16	1
Símbolo hexadecimal	**A**	**C**	**7**	**3**
Valor decimal del símbolo	10	12	7	3
Valor correspondiente	40960	3072	112	3

El valor hexadecimal AC73 es 44147 en decimal.

AC73(16) = 44147(10)

Conversión de hexadecimal (base 16) a binario (base 2)

Para pasar de hexadecimal a binario, simplemente basta con coger un cuarteto (agrupación de 4 bits), de donde se obtiene un símbolo hexadecimal.

Así, para transformar en binario **FE 87**, hay que tratar los símbolos por separado y sumar el resultado obtenido.

Si se cuenta en binario y se desea obtener la traducción hexadecimal, se obtienen los siguientes valores:

0000 0

0001 1

0010 2

0011 3

0100 4

0101 5

0110 6

0111 7

1000 8

1001 9

1010 A

1011 B

1100 C

1101 D

1110 E

1111 F

Así pues, FE 87 se escribe en binario 1111 1110 1000 0111.

A la inversa sería tan sencillo como traducir un valor binario en hexadecimal identificando los cuartetos.

Tomemos como ejemplo el número 100101011010110; primero se tendrá que descomponer en cuartetos leyendo los valores de derecha a izquierda completando según se necesite la parte «significativa» para obtener un cuarteto completo:

100 1010 1101 0110 se completará así 0100 1010 1101 0110.

A continuación 0100 se convierte en 4.

1010 se convierte en 10, en hexadecimal «A».

1101 se convierte en 13, en hexadecimal «D».

0110 se convierte en 6.

La traducción es 4A D6.

Glosario

ADSL — *Asymmetric Digital Subscriber Line*
Es una tecnología que permite conectar, a través del clásico cable telefónico de cobre, equipos (en el abonado y en la central telefónica) que permiten velocidades asimétricas de entre 512 Kbps y 1 Mbps de bajada (*download*) y 256 Kbps de subida (*upload*).

AFP — *Apple Filing Protocol*, antiguamente AppleTalk Filing Protocol
Protocolo histórico de acceso a archivos en entorno Apple. Desde Mac OS X, también se puede utilizar CIFS o FTP.

AfriNIC — *African Network Information Centre*
Uno de los cinco RIR encargados de asignar los recursos de Internet.

AH — *Authentication Header*
Es un protocolo utilizado por IPsec que permite firmar tramas, es decir, certificar su integridad y, en consecuencia, su autenticidad (no modificación).

ANSI — *American National Standards Institute*
Es un organismo americano que ha originado numerosas normas informáticas y de redes.

APIPA — *Automatic Private IP Addressing*
Es un mecanismo de asignación automática de direcciones en el rango 169.254.*.* para los clientes DHCP Microsoft que no pueden obtener direcciones IP.

APNIC — *Asia Pacific Network Information Centre*
Uno de los cinco RIR encargados de asignar los recursos de Internet.

ARIN — *American Registry for Internet Numbers*
Uno de los cinco RIR encargados de asignar los recursos de Internet.

ARP — *Address Resolution Protocol*
Es un protocolo utilizado en TCP/IP para resolver una dirección IP en dirección física.

ARPANET — *Advanced Research Project Agency NETwork*
Primera red de conmutación de paquetes, origen de Internet y desarrollada por el departamento de defensa americano.

ATM — *Asynchronous Transfer Mode*
El ATM o TTA, *Técnica de Transferencia Asíncrona*, es una forma de conmutación de celdas que proporciona velocidades muy altas.

AUI — *Access Unit Interface*
Es el conector DB15 que se utiliza para conectar una tarjeta 10 base 5 a un emisor-receptor externo.

BGP — *Border Gateway Protocol*
Protocolo externo de intercambio de tablas de enrutamiento entre sistemas autónomos.

BL — *Bucle Local*
Es la parte de la *Red Telefónica Conmutada* (RTC) situada entre el abonado y los conmutadores del proveedor de telefonía.

BLR — *Bucle Local de Radio*
Tecnología que sustituye los cables telefónicos por ondas de radio

y que solo se puede utilizar en los últimos kilómetros de la instalación.

Bluetooth Es una tecnología de red inalámbrica basada en el chip del mismo nombre.

BNC *British Naval Connector*
Es un tipo de conector utilizado en 10 base 2 para conectar un cable coaxial fino a una tarjeta de red Ethernet.

BPDU Tramas intercambiadas que permiten gestionar la topología y el algoritmo de Spanning Tree (neutralización de los bucles de nivel 2 en una red Ethernet).

BSD *Berkeley Software Development*
Es un editor de programas informáticos, origen de la versión de UNIX que proporcionó las fuentes TCP/IP gratuitamente a las universidades y que contribuyó, gracias a su difusión, al desarrollo de TCP/IP.

CCITT *Comité Consultatif International Télégraphique et Téléphonique*
Este organismo fue sustituido por la UIT.

CDDI *Copper Distributed Data Interface*
Esta norma, similar a FDDI, se basa en el cable de par trenzado como soporte de transmisión.

CHAP *Challenge Handshake Authentication Protocol*
Es un protocolo de autenticación utilizado por PPP que permite el cifrado de las contraseñas.

CIDR *Classless Inter Domain Routing*
Es un conjunto de especificaciones que permite definir la asignación de IP de un modo jerárquico en un entorno de interconexión, también jerárquico. Su objetivo es optimizar la asignación de los tramos de direcciones IP disponibles que dependen de una máscara de tamaño variable.

CIFS *Common Internet File System*
Sistema de archivos Microsoft basado en el protocolo SMB (*Session Message Block*).

CODEC *COdificador DECodificador*
Es un componente que permite convertir una fuente analógica en una señal digital.

CRC *Cyclic Redundancy Code*
Es un código de control de errores, calculado y transmitido con la trama para disponer de un primer nivel de detección de errores.

CSMA/CA *Carrier Sense Multiple Access/Collision Avoidance*
Es el método de acceso para el soporte utilizado en las redes AppleTalk. Se basa en evitar las colisiones reservando el canal antes de transmitir los datos.

CSMA/CD *Carrier Sense Multiple Access/Collision Detection*
Es el método de acceso para el soporte utilizado en las redes Ethernet. Se basa en la detección de las colisiones aun sin reservar del canal para transmitir los datos.

DAD *Duplicate Address Detection*
Protocolo utilizado en IPv6 para la autoasignación de dirección de red local.

DCE *Data Communications Equipment*

Ver ETCD.

DDoS *Distributed Denial of Service*
Denegación de servicio distribuido, corresponde a un ataque a un servicio de red que consiste en una saturación a partir de numerosas llamadas al servicio desde numerosos ordenadores. El resultado es que el servicio no puede responder durante un tiempo que puede llegar a ser importante.

DES *Data Encryption Standard*
Algoritmo de codificación de datos.

DHCP *Dynamic Host Configuration Protocol*
Es un servicio que permite asignar dinámicamente parámetros TCP/IP a los clientes que hacen el requerimiento.

DMA *Direct Memory Access*
El mecanismo de acceso directo a la memoria permite transferir información de los procesos del sistema utilizando el bus del ordenador sin sobrecargar el procesador.

DMZ En informática corresponde a una subred dentro de un cortafuegos, situada generalmente entre la red local e Internet. Este sitio alberga los servidores que serán accesibles desde Internet pasando por el cortafuegos externo generalmente a través de un mecanismo de traducción de direcciones o de puerto.

DNS *Domain Name System*
Es un servicio disponible en un entorno TCP/IP, que permite resolver nombres del tipo www.eni.fr en dirección IP.

DoS *Deny of Service* o *Denial of Service*
Es un forma común de ataque, la denegación del servicio, que consiste en saturar un recurso de un servidor para neutralizar su buen funcionamiento; por ejemplo, saturar las conexiones TCP disponibles, el procesador, el espacio en disco o incluso la red a la que se conecta el servidor.

DSLAM *Digital Subscriber Line Access Multiplexer*
O multiplexor de acceso a una línea de abonado digital, que conecta los datos que provienen del bucle local del abonado y la red ATM o Ethernet al ISP. El multiplexado permite extraer datos de Internet, televisión o voz IP.

DTE *Data Terminal Equipment*
Ver ETTD.

ESP *Encapsulating Security Payload*
Es el protocolo utilizado por IPsec para cifrar el contenido de los datos encapsulados (Payload).

ETCD *Equipamiento Terminal de Circuito de Datos*
Es un componente intermedio en un intercambio entre ETTD.

ETTD *Equipamiento Terminal de Tratamiento de Datos*
Es el componente final en un intercambio que utiliza los ETCD.

Ext2 y **Ext3** Son sistemas de archivos seguros, generalmente utilizados por los sistemas operativos Linux. Ext3 es una versión con registro diario de Ext2.

FAT *File Allocation Table*
La tabla de asignación de archivos es una de las estructuras utilizadas en los entornos OS/2, MsDOS, Windows 95 y Windows NT. Su estructura interna se basa en un encadenamiento de la

información sin introducción de índices internos para permitir optimizar los accesos.

FC *Fibre Channel*
Designa el conjunto de protocolos relativos a la interconexión SAN.

FCoE *Fibre Channel over Ethernet*
Designa la adaptación del protocolo FC para los SAN encapsulado en Ethernet.

FDDI *Fiber Distributed Data Interface*
Es una norma Token Ring que circula a 100 Mbps, que se basa en una topología lógica de doble anillo sobre fibra óptica.

FTP *File Transfer Protocol*
Protocolo de transferencia de archivos en modo seguro; se utiliza en entornos TCP/IP.

GPRS *General Packet Radio Service*
Es un sistema de transferencia de datos en telefonía móvil, también llamado generación 2.5.

GRE *Generic Routing Encapsulation*
Es un protocolo utilizado por PPTP que permite encapsular los datos en PPP para aprovechar la funcionalidad de codificación de este último.

GSM *Global System Mobile*
GSM es el primer sistema digital de telefonía móvil.

HACMP *High Availability Cluster MultiProcessing solution Cluster*
Solución de alta disponibilidad ofrecida por IBM en AIX.

HBA *Host Bus Adapter*
Identifica una interfaz de acceso a una red Fibre Channel (tarjeta de red).

HDLC *High level Data Link Control*
Es una subcapa que opera en la capa de conexión y que ofrece varios niveles de servicios. Se encuentra, principalmente, en conexiones WAN de punto a punto.

HDSL *High bit-rate Digital Subscriber Line*
Línea digital de abonado de alta velocidad que ofrece velocidad simétrica (subida y bajada) a 2 Mbps a una distancia de 3,6 kilómetros.

HSDPA *High Speed Downlink Packet Access*
Nueva generación de telefonía basada en UMTS. Es más rápida y también se denomina 3G+.

HSRP *Hot Standby Router Protocol*
Protocolo propietario CISCO que permite gestionar una dirección IP de puerta de enlace virtual asociando dos direcciones IP físicas en modo activo/pasivo.

HTML *HyperText Markup Language*
Lenguaje para la publicación de datos mediante la realización de presentaciones en modo gráfico a través de un navegador de Internet.

HTTP *HyperText Transfer Protocol*
Protocolo de transferencia de archivos que permiten manejar todo tipo de información.

HTTPS *HTTP Secure*

Es la versión HTTP que utiliza SSL para el cifrado de datos en los intercambios entre un cliente y un servidor Web.

IaaS *Infrastructure as a Service*
Concepto utilizado en la jerga del Cloud Computing para identificar una infraestructura dinámica adaptable a la demanda.

ICA *Independent Computing Architecture*
Es un protocolo utilizado por Citrix para clientes ligeros, que permite trabajar a distancia y en modo gráfico a través de una conexión de baja velocidad (solo se necesitan entre 15 y 20 Kbps en la conexión), que además ofrece compresión y cifrado de los datos de intercambio.

ICMP *Internet Control Message Protocol*
Es un protocolo básico que permite dar servicios a la gama de protocolos TCP/IP, principalmente para prevenir la pérdida de paquetes.

IDS *Intrusion Detection System*
Son sistemas, hardware o software, que se colocan en las redes para optimizar la subida de información excepcional.

IEEE *Institute of Electrical and Electronics Engineers*
Es el organismo de normalización que se encarga de las normas importantes para redes, relativas a las capas bajas.

IETF *Internet Engineering Task Force*
El objetivo de este organismo es mejorar la red de Internet.

IMAP *Internet Message Access Protocol*
Es un protocolo optimizado que permite administrar el correo electrónico a distancia. Permite que se carguen solo las cabeceras de los mensajes para poder eliminarlos sin tener que descargarlos, sobre todo en el caso de mensajes voluminosos o indeseables, al contrario de como funciona POP.

IPBX *IP Branch eXchanger*
Se trata generalmente de un servidor de aplicaciones que hace la misma función que un PABX en un entorno de voz IP (VoIP).

IPNG *Internet Protocol Next Generation*
Es la nueva generación de IP, la versión 6 (IPv6).

IPsec *IP Security*
Es un protocolo que permite aplicar el cifrado de datos en los intercambios de información en tráfico, ya sea en modo transporte o en modo túnel (en una VPN L2TP).

IPX *Internetwork Packet Exchange*
Es un protocolo de niveles de Red y Transporte, enrutable y no seguro, que se utiliza en entornos Novell.

IRDA *Infra Red Data Association*
Es un conjunto de especificaciones que permite la conexión de dispositivos de infrarrojos.

IRDP *ICMP Router Discovery Protocol*
Protocolo de descubrimiento de puertas de enlace que se basa en mensajes ICMP (*Internet Control Message Protocol*).

ISATAP *Intra-Site Automatic Tunnel Addressing Protocol*
Es un protocolo que permite la implementación automática de un túnel IPv6, entre dos sitios interconectados en IPv4.

ISO Es un organismo de normalización, mundialmente reconocido y que

administra numerosas normas.

ISP *Internet Service Provider*

Organismo proveedor de acceso a Internet, pasarela entre los clientes.

L2TP *Layer 2 Tunneling Protocol*

Es un protocolo complejo que permite poner en marcha una VPN (*Virtual Private Network*) configurando las funcionalidades (firma de las tramas con AH, cifrado de los datos con ESP, complejidad de la clave de cifrado utilizada, renovación de la clave de sesión...).

LACNIC *Latin American and Caribbean Internet Address Registry*

Uno de los cinco RIR encargados de asignar los recursos de Internet.

LAN *Local Area Network*

Red de amplitud geográfica limitada.

LIR *Local Internet Registries*

Identifica un organismo local encargado de administrar la asignación de recursos de Internet a nivel local de un país.

LLC *Logical Link Control*

Capa de nivel inferior de conexión del modelo OSI introducida por el IEEE y que ofrece distintos tipos de servicios.

LPD *Line Printer Daemon*

Es un servicio de impresión específico de TCP/IP, disponible para distintas plataformas.

LUN *Logical Unit Number*

Identificador lógico utilizado para asignar una unidad de almacenamiento.

MAC *Medium Access Control*

Capa inferior del nivel de Conexión del modelo OSI introducida por el IEEE. Administra el acceso al soporte físico integrando así el método de acceso al soporte y el direccionamiento físico.

MAN *Metropolitan Area Network*

Red cuyo alcance geográfico es relativamente amplio, a escala de una ciudad.

MAU o **MSAU** *MultiStation Access Unit*

Nombre de un concentrador Token Ring.

MFP *Multi Function Printer*

Término inglés que designa una impresora multifunción (impresora, fotocopiadora, escáner y a veces fax).

MIB *Management Information Base*

Es la estructura de datos establecida por un agente SNMP para poner a disposición información específica de un componente distribuido, hardware o software.

MÓDEM *MOdulador DEModulador*

Ejemplo de ETCD, o de equipo intermedio, que permite transmitir datos digitales en forma de señal analógica.

MPLS *Multi-Protocol Label Switching*

Esta norma de IETF se destina al transporte eficaz de las comunicaciones de red de gran envergadura.

MTU *Maximum Transfer Unit*

Es la longitud máxima de una trama en una red de nivel 2. Esta información es importante, ya que es utilizada por la IP para saber si un paquete se debe dividir o no al pasar a través de un router.

NAS *Network Attached Storage*
Sistema dedicado al almacenamiento de los datos en una red.

NAT *Network Address Translation*
Es un mecanismo que permite traducir sistemáticamente los paquetes modificando las cabeceras IP, es decir, TCP y UDP para proteger los equipos de la red interna.

NCP *Netware Core Protocol*
Protocolo de múltiples funciones, como la de proporcionar acceso a archivos e impresoras para clientes Novell.

NDIS *Network Device Interface Specification*
Es una especificación Microsoft/3Com que se utiliza en los sistemas operativos de Microsoft para los controladores de tarjetas de red y para los protocolos de capas medias.

NDP *Neighbor Discovery Protocol*
Protocolo que realiza cierto número de operaciones en IPv6, entre las cuales podemos destacar la detección de direcciones duplicadas (DDD).

NetBEUI *NetBIOS Extended User Interface*
Son dos capas de los niveles de Red y Transporte, en el sentido de OSI, que permiten disponer de capas medias intercambiables para NetBIOS (nivel de sesión).

NetBIOS *Network Basic Input/Output System*
Es una interfaz de programación para aplicaciones de red, disponible para aplicaciones cliente/servidor en cualquier protocolo de capas medias.

NetBT o **NBT** *NetBIOS over TCP/IP*
Es una versión de NetBIOS que se basa en TCP/IP.

NFS *Network File System*
Es un servicio para archivos de red en TCP/IP, que permite ver una estructura remota como si se tratase de un directorio de estructura local.

NIR *National Internet Registries*
Identifica un organismo nacional encargado de administrar la asignación de recursos de Internet a nivel de un país.

NLB *Network Load Balancing* o Balanceador de carga de red.
Es una solución que consiste en aplicar un equilibro de carga de red en un componente informático que se combina con el controlador de la tarjeta de red. Esta funcionalidad solo está disponible en algunos sistemas operativos como Windows 2000 Advanced Server.

NNTP *Network News Transfer Protocol*
Es un protocolo que permite el acceso al intercambio de correos electrónicos centralizados más conocidos como foros de discusión.

NTFS *New Technology File System*
Sistema de archivos de 64 bits, transaccional, seguro e implementado con Windows NT.

NTP *Network Time Protocol*
Es un protocolo utilizado para sincronizar el reloj de un ordenador

con el de un servidor de Internet.

ODI *Open Data Interface*
Es una especificación escrita por Novell/Apple para los controladores de tarjetas y protocolos de red, en un entorno Novell.

OSF *Open Software Foundation*
Es una fundación que permite aprovechar la experiencia de distintos proveedores. Principalmente es el origen de OSF/Motif, una interfaz gráfica de usuario.

OSI *Open System Interconnection*
Es el modelo de siete capas de referencia de la ISO.

OSPF *Open Shortest Path First*
Es un algoritmo de enrutamiento dinámico implementado por IP.

PaaS *Platform as a Service*
Concepto utilizado en la jerga del cloud computing para identificar una plataforma de desarrollo adaptable a la demanda.

PABX *Private Automatic Branch eXchange*
Commutador telefónico privado que permite conectar puestos telefónicos de una red interna de una empresa con los de la red telefónica pública (líneas externas).

PAD *Packet Assembler/Disassembler*
Es un conmutador que proporciona acceso directo a X.25.

PAN *Personal Area Network*
Red de pequeño alcance, centrada en el usuario.

PAP *Password Authentication Protocol*
Es un protocolo sencillo, que utiliza principalmente PPP y que permite efectuar una autenticación simple con un nombre de usuario y una contraseña sin encriptar (no protegida).

PING *Packet INternet Groper*
Es una herramienta de prueba de conectividad, generalmente empleada en TCP/IP para identificar un problema de enrutamiento o de configuración IP.

PNA *Program Neighborhood Agent*
Corresponde al cliente Citrix y permite administrar la virtualización de sesión y de aplicación.

POP *Post Office Protocol*
Es un protocolo muy utilizado que permite el acceso a un servidor de correo para descargar el contenido de su buzón. En algunos casos, IMAP lo puede sustituir aportando algunas ventajas.

PPP *Point to Point Protocol*
Protocolo WAN que trabaja sobre las dos primeras capas del modelo OSI, frecuentemente utilizado para conectarse a Internet.

PPPoE *Point to Point Protocol over Ethernet*
Es un protocolo de conexión Punto a Punto desarrollado específicamente para ADSL. Evita que todos los abonados se vean en el mismo soporte físico.

PPTP *Point to Point Tunneling Protocol*
Es un protocolo que permite, a través de una conexión IP multipunto, administrar una comunicación privada y segura.

RADIUS *Remote Authentication Dial In User Service*

Conjunto de funcionalidades agrupadas en un servicio que permite realizar tres tipos de acciones: la autenticación, la autorización y el inicio de sesión. Históricamente, RADIUS fue concebido para permitir a los ISP autenticar el acceso por módem de sus clientes.

RAID *Redundant Array of Inexpensive Disks*

Funcionalidad